Azienda Ospedaliero Universitaria Careggi

Valutazione d'Impatto sulla Protezione dei dati (Data Protection Impact Assestment)

Servizio Sanitario della Toscana

La DPIA (Data Protection Impact Assestment) – o anche VIP (Valutazione d'Impatto Privacy) - è un processo (che esita in un documento) inteso a descrivere il trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento, valutando detti rischi e determinando le misure per affrontarli. E' strumento e conseguenza della responsabilizzazione del titolare, e si riferisce a un trattamento conosciuto analiticamente e descritto in ogni suo aspetto; essa, perciò, assume anche una valenza organizzativa, con positiva ricaduta sul piano operativo e logistico dello studio, in particolare se osservazionale (uno studio, cioè, che si risolve esclusivamente nella raccolta ed elaborazione di dati per lo più personali. La DPIA mette dunque a disposizione, in generale:

- 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[1] e oggetto di parere da parte del Responsabile della protezione dei dati.

DESCRIZIONE DEL TRATTAMENTO DEI DATI

Impatto dello spread through air space (STAS) sulla sopravvivenza nei pazienti affetti da tumore polmonare primitivo sincrono multiplo bilaterale (SPBLC)

L'obiettivo primario è quello di valutare la presenza di fattori prognostici di aumentata sopravvivenza e intervallo libero da malattia (disease-free survival DFS) in pazienti con tumori polmonari primitivi sincroni e multipli (MPLC); valutare l'impatto dello Spread Through Air Space (STAS) nella sopravvivenza di pazienti con tumori polmonari sincroni e multipli trattati chirurgicamente e di valutare l'influenza della presenza di tumore del polmone primitivo sincrono e multiplo sulla sopravvivenza globale a distanza (overall survival - OS-) e cancro-specifica (cancer-specific survival CSS) oltre alla sopravvivenza libera da malattia (disease free survival DFS)

Le variabili di interesse sono:

Preoperatorie: età, sesso, bmi, performance status secondo ECOG, comorbilità, comorbidity index, FEV1%, FVC%, DLCO% (dati valutati prima di entrambi gli interventi chirurgici) smoking history (former, actual, never), pack years, stadio clinico, pattern T, pattern N, pattern M, dimensioni T (dati valutati prima di entrambi gli interventi chirurgici), pattern radiologico lesione principale e seconda lesione (solido, part-solid, ground glass), SUV lesione principale e seconda lesione

Chirurgia: data intervento gg/mm/aaaa, tipo intervento, approccio, tipo di linfoadenectomia, durata, margini chirurgici. I dati sono valutati per entrambi gli interventi chirurgici eseguiti sul singolo paziente.

Post-operatorie: degenza, degenza in ICU, complicanze, mortalità, durata drenaggio, diagnosi istopatologica, subclassificazione adenocarcinoma, stadio patologico, pattern T, pattern N, pattern M, dimensioni patologiche, STAS, R, assetto biomolecolare ed immunoistochimico, margini patologici. I dati sono valutati per entrambi gli interventi chirurgici eseguiti sul singolo paziente.

A distanza: data decesso, causa decesso, data recurrence, sito di recurrence, terapie post-chirurgiche

Le persone fisiche interessate al trattamento saranno tutti i pazienti adulti (<18 anni), affetti da **Synchronous primary bilateral lung carcinomas (SPBLC)***, sottoposti trattamento chirurgico bilaterale con tecniche mininvasive o OPEN.* Considerando la mole di attività della SOD Chirurgia Toraco-Polmonare ed il periodo di studio, potranno essere interessati al trattamento circa 60 soggetti.

Dott. Stefano Bongiolatti, medico chirurgo, promotore dello studio e principal investigator
Prof. Luca Voltolini, medico chirurgo, cp-investigator

Nessun soggetto esterno

I dati saranno raccolti dalla cartella elettronica (software Archimed/Archiamb) ed inseriti sulla piattaforma web REDCap in maniera pseudonimizzata da parte dello sperimetatore principale o da parte dei co-investigator che avranno una password personale per accedere alla piattaforma di inserimento dei dati.

- I dati di interesse saranno trascritti in un database di studio ospitato sulla piattaforma RedCap
- Nel database i dati saranno inseriti prevedendo che ciascun paziente sia indicato da un codice personale (Subject ID), utilizzando un criterio di pseudonimizzazione
- I dati saranno archiviati e conservati per un periodo di almeno 7 anni.
- Verrà utilizzata la piattaforma RedCap per la raccolta dei dati, con accesso vincolato da user e password temporanei in possesso dei soli soltanto agli sperimentatori coinvolti nello studio.
- I dati vengono estrapolati mediante apposita funzione presente su RedCap e denominata "data export tool" che permette, dopo l'attribuzione di un codice univoco randomico, di esportare tutti i dati o effettuare una selezione di quelli d'interesse nella modalità di fruizione per l'analisi. L'estrazione dei dati prevederà la consultazione dei sistemi operativi dell'AOUC e delle cartelle dei pazienti e la trascrizione dei dati di interesse nella piattaforma deputata alla raccolta dei dati dello studio.

I dati sono accessibili con modalità unica attraverso credenziali e password personale per ogni Data Entry Person. L'accesso alla visualizzazione dei dati pseudo-anonimizzati dipende dai privilegi che vengono assegnati dal PI al momento della registrazione allo studio sul portale RedCap.

I dati saranno archiviati sulla piattaforma web REDCap

PRINCIPI FONDAMENTALI[2]

La base giuridica del trattamento è il consenso. Per gli interessati che non sarà possibile informare e per i quali non sarà possibile ottenere il consenso, è rappresentata, dal parere positivo del competente comitato etico a livello territoriale *(e* la successiva autorizzazione del Direttore Generale dell'AOUC), alla luce della nuova formulazione dell'art. 110 del D.Lgs. 30 giugno 2003 n. 196 Codice in materia di protezione dei dati personali, conseguente alle modifiche apportate dalla Legge 56 del 29 aprile 2024

I dati raccolti sono esclusivamente quelli indispensabili al raggiungimento degli obiettivi dello studio

I dati saranno conservati per 7 anni dalla fine dello studio che sarà prevista per dicembre 2025.
Considerato 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 non assente, comunque non direttamente ed immediatamente prescrittiva - così che viene comunque chiamata in causa la responsabilizzazione del Titolare - si è considerato opportuno applicare a questo studio osservazionale il termine già previsto dal D.Lgs. 6 novembre 2007, n. 200, riferibile ad una prassi consolidata e soprattutto ritenuto sufficiente e non eccedente allo scopo di consentire eventuali controlli successivi sulla correttezza delle inferenze effettuate nella valutazione dei dati raccolti nel corso della ricerca.

Verrà effettuato un doppio controllo sui dati inseriti da parte del personale coinvolto nello studio.
L'utilizzo della piattaforma REDCap garantisce una Stretta profilazione degli accessi, pseudonimizzazione dei dati, cifratura del database.
Le modalità di pseudonimizzazione dei dati avverranno attraverso l'assegnazione di un codice numerico (Subject ID). I dati personali sono trattati in associazione con questa informazione non direttamente identificativa, e la correlazione tra questa e i dati identificativi dell'interessato è conservata separatamente, accessibile al solo personale coinvolto nello studio, assicurandone, con idonee misure di sicurezza tecniche ed organizzative, la riservatezza. Il Subject ID consisterà in un codice numerico progressivo, generato ogni qual volta un nuovo paziente viene arruolato nello studio
L'accesso e il trasferimento dei dati da e verso la piattaforma REDCap sono gestiti con protocollo https e Crittografia a 128 bit con certificato SSL a doppia chiave e mantenuti con Crittografia AES 128 (una connessione sicura con trasferimento dati crittografato).
I dati sono anonimizzati prima della pubblicazione, secondo la tecnica della K anonimizzazione prevedendo un valore K pari a 4
Nessun differente profilo per gli sperimentatori
Gli accessi alla piattaforma REDCap sono tracciati.
Il backup dei dati verrà effettuato settimanalmente in un archivio protetto da password e alla fine dello studio e vista la sua natura retrospettiva non sarà più possibile inserirne di nuovi.
Tutti i computer sono aggiornati all'ultima versione del sistema operativo e sono dotati di efficaci software antivirus aggiornati volti a contrastare eventuali attacchi da parte di virus e malware.
I dati non saranno gestiti su supporti cartacei.
DIRITTI DEGLI INTERESSATI
Ai pazienti che sono in vita e che si presenteranno alle visite ambulatoriali verrà consegnata una informativa redatta ai sensi dell'art. 13 del Regolamento. Per i pazienti che non si presenteranno alle visite ambulatoriali, essi saranno informati telefonicamente e quindi oralmente in maniera esaustiva dal principal investigator o dai co-investigator.
Il consenso informato non sarà applicato agli interessati quando i soggetti non risulteranno contattabili (tre tentativi di contatto telefonico o mancata risposta ad email per 15 gg).

Nel corso della prima visita ambulatoriale, dopo che lo studio sarà stato approvato, verrà acquisito il consenso informato.

Ove applicabile: indicare se il trattamento coinvolge soggetti qualificati come responsabili del trattamento[3]
N.A

GESTIONE DEI RISCHI[4]

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

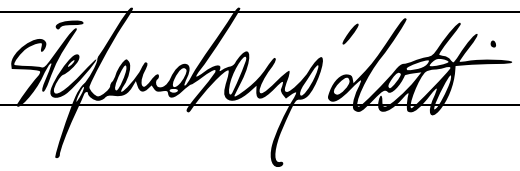
PERDITA DEI DATI

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

IL PREPOSTO AL TRATTAMENTO
Dott. Stefano Bongiolatti

FIRMA 	*Data* 01/09/2025

[1]Il Preposto al trattamento, in Azienda, è, per quanto riguarda gli studi, il PI.
L'art. 2-quaterdecies del D.Lgs. 30 giugno 2003 n. 196 prevede che, tra le persone autorizzate al trattamento (cfr. nota 6), il titolare possa individuare, per lo svolgimento di specifiche funzioni di coordinamento e orientamento nel trattamento dei dati, persone fisiche, che operano sotto la loro autorità, a ciò "espressamente designate". La persona fisica "espressamente designata", che coincide con la vecchia nozione di "responsabile interno del trattamento" (oggi il responsabile del trattamento è solo un soggetto esterno), è stata sinteticamente ridenominata dai diversi titolari, utilizzando varie espressioni (delegato, referente ecc.): in Azienda la si è definita *Preposto*, con termine derivato dalla normativa in materia di sicurezza del lavoro, e che indica appunto un soggetto che sovraintende ad una data attività (a far intendere che il trattamento dei dati non è mai una attività sganciata da un concreto operare).
[2]L'art. 5 (*Principi applicabili al trattamento di dati personali*) par. 1 del Regolamento prescrive analiticamente alcuni principi che assicurano l'adeguatezza del trattamento (cd. *principi base del trattamento*); la *responsabilizzazione* del Titolare consiste appunto nel rispettare tali principi e nell'essere in grado di dimostrare, con idonea documentazione (redatta prima dell'inizio del trattamento, nell'ottica della privacy by design e by defaut) di averli rispettati. Dunque, il titolare del trattamento è responsabile del rispetto dei seguenti principi:

- limitazione della finalità del trattamento;
- limitazione della conservazione dei dati,
- minimizzazione dei dati;
- esattezza dei dati;
- sicurezza dei dati (integrità e riservatezza).
- trasparenza del trattamento (riguarda anzitutto le informazioni sul trattamento messe a disposizione degli interessati, se ne parla alla sezione successiva relativa ai Diritti degli interessati)

[3]E' Responsabile del trattamento il soggetto esterno rispetto al titolare che tratta dati per conto – cioè per le finalità – del titolare, secondo le modalità da questo indicate. Ai sensi dell'art. 28 paragrafo 3 del Regolamento tale incarico deve essere formalizzato in un contratto o altro atto giuridico, che precisi la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento; tale atto deve essere redatto in modo tale che il responsabile tratti i dati personali soltanto su istruzione documentata del titolare del trattamento.
[4]La parte conclusiva della DPIA, dopo la descrizione del trattamento e delle misure tecnico-organizzative individuate a garanzia della sua adeguatezza, è quella propriamente dedicata alla valutazione circa la sostenibilità dei rischi individuati. Tali rischi si articolano in riferimento alla perdita:

- di riservatezza dei dati
- di integrità dei dati
- di disponibilità dei dati

La stima conclusiva della probabilità e gravità di ogni tipologia di rischio è da indicarsi nei seguenti termini:

- indefinita
- trascurabile
- limitata
- importante
- massima.

Ogni valutazione sintetica deve essere adeguatamente motivata.

Qualora si utilizzi REDCAP; è possibile limitarsi indicare quanto segue:

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 ai 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.