



La DPIA (Data Protection Impact Assessment) – o anche VIP (Valutazione d'Impatto Privacy) - è un processo, che si risolve in un documento, 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 trattamentoⁱ e oggetto di valutazione del Responsabile della protezione dei dati.

DESCRIZIONE DEL TRATTAMENTO DEI DATI

Denominazione del trattamentoⁱⁱ

Evaluation of oncological outcomes in multifocalhepatocellular carcinoma

Indicare la finalità del trattamentoⁱⁱⁱ

Lo studio si propone l'obiettivo di valutare gli outcomes oncologici (sopravvivenza globale e libera da malattia) dei pazienti sottoposti ad intervento chirurgico, open o mininvasivo, per epatocarcinoma (HCC) multifocale.

Indicare le tipologie di dati oggetto del trattamento,specificando ogni tipologia di dato^{iv}

- Dati anagrafici: Età, BMI, Genere, ASA
- Dati riguardanti esiti degli esami radiologici (TC e RM): numero e sede del tumore, caratteristiche radiologiche del tumore (comportamento dopo somministrazione del mezzo di contrasto), presenza di altre sedi di malattia
- Dati riguardanti l'esito degli esami ematici: emocromo con formula, INR, bilirubina, creatinina, piastrine, albumina, Alfafetoproteina.
- Dati anamnestici: Cirrosi (sì/no), diabete (sì/no), cardiopatia (sì/no), varici (sì/no), Child-Pugh score, MELD score ed ALBI score, Eziologia della malattia epatica: virale, alcolica, dismetabolica, mista o altra
- Dati riguardanti il trattamento del paziente: Intervento chirurgico (open/mininvasivo), complicanze post procedurali (sì/no), grading delle complicanze secondo la classificazione di Clavien-Dindo, Durata della degenza ospedaliera
- Dati riguardanti l'esame istologico del pezzo operatorio: Numero e diametro delle lesioni, Risposta istopatologica: pTNM, grading, numero dei noduli, dimensioni, margini.
- Dati riguardanti eventuali terapie neo/-adiuvanti: Tipo di terapia neo-/adiuvante, durata, restaging
- Dati relatici alla recidiva/ripresa di malattia: Recidiva (sì/no), data della recidiva, decesso (sì/no), data del decesso, Sopravvivenza libera da malattia, sopravvivenza globale

Indicare le tipologie di interessati al trattamento^v

Pazienti affetti da epatocarcinoma che sono stati ricoverati/visitati presso le SOD di Chirurgia epato-bilio-pancreatica da Gennaio 2017 a Dicembre 2024.

Indicare i soggetti interni che partecipano al trattamento quali persone espressamente designate o autorizzate e se queste siano state adeguatamente istruite sul trattamento^{vi}

Oltre al PI dello studio, Prof. Gian Luca Grazi, fanno parte del gruppo di studio altri 2 medici afferenti alla SOD Chirurgia epato-bilio-pancreatica

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^{vii}



Nessun soggetto esterno parteciperà al trattamento

Descrivere il flusso dati (cioè come i dati sono spostati o elaborati). Occorre descrivere il flusso analiticamente nei suoi vari passaggi, operazioni, attori^{viii}
I dati saranno raccolti dalle cartelle cliniche informatizzate dei pazienti (Archimed), dal programma esami di laboratorio (nuovoDNweb), dal programma referti anatomia patologica aziendale (Spartito), dal programma registro operatorio aziendale (Ormaweb), dai registri delle regolari visite di follow-up, dal programma di registrazione delle visite ambulatoriali aziendali (AMBU), programma di registrazione visite oncologiche aziendali (Oncosys), colloquio telefonico con il paziente.
I dati ottenuti vengono progressivamente inseriti nell'applicativo RedCap prevedendo che per ciascun paziente sia indicato un codice personale. I dati verranno poi estratti sotto forma di file Excel e inseriti su un programma per l'analisi statistica (SPSS Statistic 30.0.0). Il file Excel verrà immediatamente cancellato.
I dati sono accessibili con modalità unica attraverso credenziali e password personale per ogni medico facente parte del gruppo di studio.

Indicare dove vengono archiviati e conservati i dati^{ix}

I dati saranno archiviati sulla piattaforma Redcap

Indicare se i dati sono trasferiti (si/no) ed eventualmente dove^x

I dati non saranno trasferiti

PRINCIPI FONDAMENTALI^{xi}

Limitazione delle finalità

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 (ela 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

Minimizzazione dei dati:

I dati raccolti (sono esclusivamente quelli necessari allo studio

Limitazione della conservazione:

I dati saranno conservati per 7 anni dalla fine dello studio prevista per Dicembre 2034.

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.



Esattezza dei dati:

Verrà effettuato un doppio controllo sui dati inseriti da parte del personale coinvolto nello studio.

Integrità e riservatezza dei dati^{xii}: 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, precisando quanto segue:

L'utilizzo della piattaforma REDCap garantisce una stretta profilazione degli accessi, pseudonimizzazione dei dati, cifratura del database

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono pseudonimizzati, e secondo quali modalità
I dati durante il loro trattamento saranno pseudonimizzati associando un codice univoco ad ogni paziente, che consisterà in un codice numerico progressivo, generato ogni qual volta un nuovo paziente viene arruolato nello studio

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono crittografati, e secondo quali modalità (ovvero quale sistema di crittografia è utilizzato)¹
Non sono previste modalità di crittografia dei dati

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono anonimizzati, e secondo quali modalità^{xiii}
I dati sono anonimizzati prima della pubblicazione

Indicare se i dati sono soggetti a partizione^{xiv}
Non è prevista partizione dei dati.

Indicare con quali misure e cautele viene effettuato il trasferimento dei dati^{xv}
Non sono previsti trasferimenti dei dati

Indicare i criteri di profilazione per l'accesso ai dati^{xvi}
Nessun differente profilo per i medici appartenenti al gruppo di studio.

Indicare se gli accessi sono tracciati^{xvii}
Gli accessi all'applicativo RedCap sono tracciati,

Indicare con quale frequenza viene effettuato il backup dei dati ed il sistema utilizzato^{xviii}
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.

Indicare se il sistema prevede misure contro virus e malware^{xix}
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.



Indicare se i dati sono trattati anche su supporti cartacei, e come questi sono gestiti^{xx}

I dati non saranno trattati su supporti cartacei

DIRITTI DEGLI INTERESSATI

Indicare come sono informati gli interessati al trattamento oppure, in alternativa, le ragioni per cui non è possibile informare gli interessati, specificando i dati di contatto del soggetto al quale gli interessati (o altri soggetti legittimati) possono indirizzare le proprie richieste relative all'esercizio dei diritti di accesso e di portabilità dei dati, dei diritti di rettifica e di cancellazione, dei diritti di limitazione e di opposizione^{xxi}

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-investigatori.

Ove applicabile: indicare come è acquisito il consenso degli interessati

La firma del consenso avverrà al momento delle visite di follow up programmate nel percorso oncologico del paziente.

Ove applicabile: indicare le ragioni per cui non è possibile informare gli interessati²³

Per motivi di impossibilità organizzativa all'esito di ogni ragionevole sforzo compiuto per contattare pazienti che al momento dell'arruolamento nello studio risultino essere deceduti o comunque non contattabili. La mancata considerazione dei dati riferiti a questi, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati. Di seguito i motivi per cui il contatto di un paziente possa rappresentare un ostacolo di impossibilità organizzativa:

- irreperibilità e/o oggettiva impossibilità organizzativa dovuta alla limitata disponibilità di indirizzi completi ed aggiornati dei pazienti;
- irreperibilità e/o oggettiva impossibilità organizzativa dovuta all'elevata percentuale di pazienti non più seguiti dal centro (di sperimentazione coinvolto);
- impossibilità organizzativa e/o di fatto dovuta alla lontananza geografica dei pazienti che rende eccessivamente difficile e costoso il loro ritorno al centro (di sperimentazione coinvolto) per le procedure di consenso, unitamente alla difficoltà di interagire con l'ausilio di strumenti elettronici da parte di pazienti anziani o aventi poca dimestichezza con le attrezzature elettroniche/informatiche;
- decesso del paziente;
- sforzo oggettivamente sproporzionato rispetto agli obiettivi dello Studio che rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

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

N.A

GESTIONE DEI RISCHI^{xxiii} (Se si utilizza Redcap)

ACCESSO ILLEGITTIMO AI DATI

Indicare, anche alla luce delle misure pianificate, una stima della probabilità e gravità del rischio (indefinita, trascurabile, limitata, importante, massima) connesso alla perdita di riservatezza dei dati, specificando, se possibile, le principali minacce che potrebbero concretizzare il rischio e le principali fonti di rischio.

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

Indicare, anche alla luce delle misure pianificate, una stima della probabilità e gravità del rischio (indefinita, trascurabile, limitata, importante, massima) connesso alla perdita di integrità dei dati, specificando, se possibile, le principali minacce che potrebbero concretizzare il rischio e le principali fonti di rischio.

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

Indicare, anche alla luce delle misure pianificate, una stima della probabilità e gravità del rischio (indefinita, trascurabile, limitata, importante, massima) connesso alla perdita di disponibilità dei dati, specificando, se possibile, le principali minacce che potrebbero concretizzare il rischio e le principali fonti di rischio.

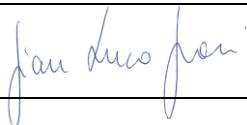
La probabilità di perdita dei dati è estremamente bassa, mentre l'eventuale danno sarebbe molto elevato.

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(vedi nota 1)
(nome/cognome)

Professor Gian Luca Grazi

FIRMA 	Data 21/03/2025
---	---------------------------



**Azienda
Ospedaliero
Universitaria
Careggi**

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



M/903/150-C
Rev. 4