



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 trattamento¹ e oggetto di valutazione del Responsabile della protezione dei dati.

DESCRIZIONE DEL TRATTAMENTO

Denominazione del trattamento

Catheter-related bloodstream infection (CRBSI) e catheter failure in cardiocirurgia: studio osservazionale retrospettivo

Indicare la finalità del trattamento

Lo scopo dello studio è quello di definire eziologia, incidenza, outcomes e fattori di rischio per CRBSI (infezioni del torrente ematico correlate ai cateteri venosi centrali), incidenza e complicanze associate a catheter failure nel setting cardiocirurgico. Descrivere l'incidenza delle infezioni correlate al catetere e della catheter failure può chiarire l'efficacia dell'attuale pratica di inserimento e gestione dei cateteri venosi centrali (CVC) nei pazienti ricoverati per essere sottoposti a un intervento cardiocirurgico.

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

Dati comuni: Età e genere.

Dati clinici: Fattori di rischio cardiovascolare e comorbidità: diabete mellito, ipertensione, ipercolesterolemia, obesità, fumo, insufficienza renale cronica. Tipo di intervento chirurgico subito. Tipo di CVC posizionato (3 lumi, 4 lumi, tecnica di inserimento ecoguidata, durata del catetere in sede, motivi della rimozione (malfunzionamento, sospetta infezione, rimozione accidentale)). Trattamento inotropo o vasocostrittore nel postoperatorio. Uso postoperatorio della CRRT. Uso dello IABP. Eventuali complicanze occorse durante il periodo perioperatorio. Eventuale decesso. Durata di degenza in Terapia Intensiva e ospedaliera.

Dati di laboratorio: Creatinina preoperatoria, Ematocrito preoperatorio. Emocolture postoperatorie, colture della punta del catetere postoperatorie.

Indicare le tipologie di interessati al trattamento

Circa 500 pazienti con età > 18 anni, sottoposti ad intervento di cardiocirurgia in urgenza o in elezione, per la cui gestione è stato posizionato un catetere venoso centrale in vena giugulare interna destra.



Indicare i soggetti interni che partecipano al trattamento quali persone espressamente designate o autorizzate e se queste siano state adeguatamente istruite sul trattamento²

Dr. Raffaele Mandarano, SOD Cardiorianimazione (Principal investigator), Dr. Sergio Bevilacqua SOD Cardiorianimazione.

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 trattamento³

Non è previsto che soggetti esterni partecipino al trattamento dei dati personali.

Descrivere il flusso dati (cioè come i dati sono spostati o elaborati). Occorre descrivere il flusso analiticamente nei suoi vari passaggi, operazioni, attori⁴.

I dati sono estratti dalla cartella clinica elettronica aziendale Archimed®, sulla base di una serie di item predefiniti, su un foglio Excel; sono quindi tolti i riferimenti anagrafici ed il numero di cartella (il numero nosologico); i dati sono quindi pseudonimizzati associando ad ogni paziente un codice alfanumerico.

Il foglio elettronico viene quindi importato nel database messo a disposizione dall'Azienda Ospedaliero Universitaria Careggi per gli studi osservazionali (Redcap®) e subito eliminato; tali dati sono quelli soggetti a conservazione per il termine stabilito. Da Redcap viene a sua volta estratto un foglio Excel che viene immediatamente trasferito sul sistema di statistica STATA. Anche tale file, una volta inseriti i dati in STATA, è subito cancellato. I dati sono oggetto, su SPSS, di valutazioni statistiche in forma aggregata. Una volta ottenuti i dati anche il file di SPSS viene cancellato, in modo che l'unico software sul quale sono conservati i dati sia RedCap®.

Indicare dove vengono archiviati i dati⁵

I dati saranno archiviati e conservati esclusivamente su supporto informatico, sul database Redcap®

Indicare se i dati sono trasferiti In dati non vengono trasferiti al di fuori dell'Azienda.

PRINCIPI FONDAMENTALI

Limitazione delle finalità: indicare la base giuridica del trattamento, cioè la sua finalità lecita, quale prevista dal Regolamento UE 2016/679 (d'ora in poi Regolamento)⁷. 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.



Minimizzazione dei dati: I dati trattati sono, sotto responsabilità del titolare dello studio, quelli strettamente indispensabili alla realizzazione dello studio ed al raggiungimento degli obiettivi sopra esposti, come esplicitato nel protocollo di ricerca.

Limitazione della conservazione:

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. 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 indiretta e non immediata, si è ritenuto opportuno applicare a questo studio osservazionale il termine dei 7 anni (già previsto dal D.Lgs. 6 novembre 2007, n. 200) in ragione del tipo di studio.

Esattezza dei dati:

I dati saranno ricontrollati uno ad uno dalla cartella clinica elettronica per verificare e correggere eventuali errori di raccolta e archiviazione.

Integrità e riservatezza dei dati: Gli utenti sono profilati e l'accesso ai database è tracciato.

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono pseudonimizzati, e secondo quali modalità¹²

I dati personali di ciascun paziente sono pseudonimizzati. La pseudonimizzazione avviene già in fase di estrazione degli stessi dati dalla cartella clinica elettronica. Le generalità dei pazienti afferenti allo studio verranno omesse e sostituite dall'assegnazione di un codice numerico sequenziale dal quale non sarà possibile in nessun modo risalire all'identità del malato se non attraverso una chiave di decodifica

(associazione tra il codice univoco e le generalità del malato) conservata in un ulteriore foglio elettronico protetto da password e custodito sotto la responsabilità dello sperimentatore principale.
Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono crittografati, e secondo quali modalità¹³ I dati non sono crittografati.
Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono anonimizzati, e secondo quali modalità¹⁴ Nella fase di pubblicazione i dati saranno riportati in modo totalmente anonimo, senza alcuna possibilità di risalire all'identità dei partecipanti.
Indicare se i dati sono soggetti a partizione¹⁵ I dati non sono sottoposti a partizione
Indicare con quali misure e cautele viene effettuato il trasferimento dei dati¹⁶ NA
Indicare i criteri di profilazione per l'accesso ai dati¹⁷ Solo lo sperimentatore principale ha accesso ai dati con un profilo di accesso di consultazione, modifica ed elaborazione dopo apertura del file dei dati.
Indicare se gli accessi sono tracciati¹⁸ Redcap® traccia gli accessi e le operazioni effettuate sui dati
Indicare con quale frequenza viene effettuato il backup dei dati¹⁹ Il backup del sistema di archiviazione e conservazione dei dati viene effettuato ogni 24 ore
Indicare se il sistema prevede misure contro virus e malware²⁰ Antivirus Aziendale AOUC
Indicare se i dati sono trattati anche su supporti cartacei, e come questi sono gestiti²¹ I dati non sono archiviati su supporti cartacei.
DIRITTI DEGLI INTERESSATI
Ove applicabile: indicare come sono informati gli interessati al trattamento Ai pazienti che si presenteranno alle visite ambulatoriali verrà messa a disposizione una informativa redatta ai sensi dell'Art. 13 del Regolamento UE 2016/679
Ove applicabile: indicare le ragioni per cui non è possibile informare gli interessati Considerato il numero elevato di pazienti inclusi nello studio, circa 500 pazienti operati dal 1 giugno 2022 al 31 dicembre 2023, e considerata anche la natura osservazionale e retrospettiva dello studio, l'arco temporale a cui si riferiscono i dati di interesse, l'età media elevata dei pazienti, i frequenti deficit cognitivi o motori, la provenienza da altre aree geografiche che rende proibitiva la loro chiamata in ospedale solo per firmare il documento di consenso, sarà resa l'informativa e richiesto il consenso agli interessati inclusi nella ricerca in tutti quei casi in cui nel corso dello studio ciò sia possibile e in particolare laddove questi si rivolgano al centro di cura, anche per visite di controllo, anche al fine di consentire loro di esercitare i loro diritti. Se i pazienti risulteranno essere deceduti o non contattabili al momento dell'arruolamento nello studio, all'esito di ogni favorevole sforzo compiuto per contattarli, non sarà acquisito il consenso per una oggettiva impossibilità di carattere organizzativo.



Ove applicabile: indicare se gli obblighi del responsabile del trattamento sono chiaramente definiti e formalizzati, e in caso di risposta positiva precisare come²²

Il trattamento non viene esternalizzato presso alcun responsabile del trattamento.

Valutare se, in caso di trasferimento dei dati al di fuori della UE, i dati godono di una protezione equivalente²³

I dati non saranno trasferiti al di fuori della UE.

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.

IL PREPOSTO AL TRATTAMENTO

Dr. Raffaele Mandarano