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
Indicare la denominazione del trattamento:[2] Fattori predisponenti, incidenza e valore prognostico dell'insorgenza di piastrinopenia in pazienti sottoposti ad impianto valvolare aortico transcatetere (TAVI). *Risk factors, incidence and outcome of Thrombocytopenia's onset after Transcatheter Aortic Valve Implantation (TAVI).*
Indicare la finalità del trattamento[3] Lo scopo dello studio è quello di evidenziare eventuale fattori prognostici e predittivi della comparsa di una complicanza comune (riduzione del numero di piastrine) successiva ad intervento di sostituzione valvolare aortica.
Indicare le tipologie di dati oggetto del trattamento, specificando ogni tipologia di dato[4] Dati anagrafici (come ad esempio età e sesso del paziente), dati anamnestici del paziente (riguardanti sia l'intervento di TAVI al quale è stato sottoposto, sia le sue patologie pregresse e la terapia in atto al momento dell'intervento) e dati clinici, laboratoristici e strumentali, afferenti al ricovero durante il quale è stato eseguito l'intervento di TAVI e che sono già previsti dalla normale pratica clinica (ad esempio dati ecocardiografici, dati laboratoristici del monitoraggio previsto post-intervento, dati clinici post-intervento come sviluppo di febbre, trombocitopenia, necessità di ulteriori interventi)
Il trattamento ricomprende l'utilizzo di strumenti di Intelligenza Artificiale? Se SI qual è la logica di funzionamento? No, non prevede utilizzo di strumenti di intelligenza artificiale.
Indicare le tipologie di interessati al trattamento[5] Pazienti sottoposti ad intervento di sostituzione valvolare aortica percutanea (TAVI) trattati presso l'AOU Careggi dal 01/01/2020 al 31/12/2025. .
Indicare i soggetti interni che partecipano al trattamento quali persone espressamente designate o autorizzate[6] Oltre al PI dello studio, la Dott.ssa Valentina Scheggi, altri 4 medici appartenenti al gruppo di studio.
Indicare eventuali soggetti esterni che partecipano al trattamento quali titolari, responsabili o persone designate/autorizzate al trattamento[7] Nessun soggetto esterno partecipa al trattamento dei dati
Descrivere il flusso dati (cioè come i dati sono spostati o elaborati). Occorre descrivere il flusso analiticamente nei suoi vari passaggi, operazioni, attori[8] I dati saranno raccolti dalla cartella elettronica aziendale denominata "Archimed" e inseriti sul database "Redcap" in maniera pseudonimizzata, assegnando a ciascun paziente un codice personale. L'accesso a Redcap è vincolato da user e password temporanei in possesso dello sperimentatore principale e dei medici

appartenenti al gruppo di studio. I dati verranno poi estrapolati mediante apposita funzione presente su Redcap e saranno poi elaborati mediante il programma statistico denominato "Spss" per eseguire le elaborazioni necessarie al fine stesso dello studio.

Indicare dove vengono archiviati e conservati i dati[9]

I dati saranno archiviati e conservati sul sistema di archiviazione aziendale RedCap.

PRINCIPI FONDAMENTALI[10]

Limitazione delle finalità: indicare la base giuridica del trattamento, cioè la sua finalità lecita, quale prevista ex artt. 6 e 9 del Regolamento UE 2016/679 (d'ora in poi Regolamento)[11]

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: indicare i criteri utilizzati per garantire l'adeguatezza, la pertinenza e la non eccedenza dei dati utilizzati[12]

I dati raccolti sono quelli indispensabili alla esecuzione dello studio.

Limitazione della conservazione: indicare per quanto tempo sono conservati i dati e i criteri per la conservazione dei dati[13]

Si è considerato opportuno applicare a questo studio osservazionale il termine di conservazione di 7 anni già previsto dal D.Lgs. 6 novembre 2007, n. 200, riferibile ad una prassi consolidata e soprattutto ritenuto sufficiente e non eccedente in relazione allo scopo di consentire eventuali controlli successivi sulla correttezza delle inferenze effettuate nella valutazione dei dati raccolti nel corso della ricerca. Il termine settennale è commisurato alla opportunità di conservare una base dati statistica per successive verifiche o richieste di precisazioni circa i risultati pubblicati.

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[14]

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

.

Integrità e riservatezza dei dati[15]: 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:

I dati sono conservati su database RedCap presente su singolo computer aziendale fisso con apposite credenziali di accesso e tenuto in apposita stanza con accesso ristretto solo ad appartenenti del gruppo di ricerca.

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono pseudonimizzati, e secondo quali modalità[16]

Le modalità di pseudonimizzazione dei dati avverrà 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.

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)[17]

I dati non sono crittografati.

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono anonimizzati, e secondo quali modalità[18]

I dati saranno anonimizzati prima della pubblicazione.

Indicare i criteri di profilazione per l'accesso ai dati[19]

Nessun differente profilo per il PI e gli altri medici appartenenti al gruppo di sperimentazione.

Indicare se gli accessi sono tracciati[20]

Gli accessi alla piattaforma REDCap sono tracciati.

Indicare con quale frequenza viene effettuato il backup dei dati[21]

Il backup dei dati viene effettuato a cadenza bisettimanale.

Indicare se il sistema prevede misure contro virus e malware[22]

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[23]

I dati non saranno gestiti su supporti cartacei.

DIRITTI DEGLI INTERESSATI

Indicare come sono informati gli interessati al trattamento[24]

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.

Indicare le ragioni per cui non è possibile informare gli interessati[25]

- decesso del paziente
- intervenuta incapacità di intendere e di volere a causa dell'aggravarsi dello stato clinico
- sforzo oggettivamente sproporzionato rispetto agli obbiettivi dello studio che rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca

Indicare, per gli studi per i quali è possibile, come è acquisito il consenso di quota parte degli interessati[26]

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

Indicare se il trattamento coinvolge soggetti qualificati come responsabili del trattamento[27]

N/A

GESTIONE DEI RISCHI[28]

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.ssa Valentina Scheggi

FIRMA	*Data* 4/2/25