Azienda Ospedaliero Universitaria Careggi

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

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 trattamentodi 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 parereda parte del Responsabile della protezione dei dati.

DESCRIZIONE DEL TRATTAMENTO DEI DATI
Indicare la denominazione del trattamento[2] ***AR**ytmic **MONI**toring after PFO **C**losure (**ARMONIC** study): Observational retrospective study by Heart and Brain outpatient clinic*
Indicare la finalità del trattamento[3] Lo *scopo dello studio è quello di andare a valutare l'incidenza di aritmie, principalmente la fibrillazione atriale, dopo la chiusura percutanea del forame ovale nei pazienti afferenti all'ambulatorio Heart and Brain coordinato congiuntamente dalla SOD Stroke Unit e Interventistica Cardiologia Strutturale dell'Azienda Ospedaliero Universitaria di Careggi (AOUC), Firenze (FI)*
Indicare le tipologie di dati oggetto del trattamento, specificando ogni tipologia di dato[4] *Dati comuni: dati anagrafici e di contatto, raccolti dai registri digitali dell'Azienda (ArchiMed e ArchiAmbu).* *Dati particolari: dati clinici, cioè relativi allo stato di salute dei soggetti, raccolti dall'anamnesi e dai referti degli esami laboratoristici e strumentali eseguiti dai soggetti sia all'interno che all'esterno dell'Azienda (nel primo caso i dati saranno visualizzabili nei registri digitali dell'Azienda, nel secondo ci verranno forniti in formato cartaceo dai diretti interessati).*
Indicare le tipologie di interessati al trattamento[5] *Gli interessati al trattamento saranno i circa 200 pazienti sottoposti a chiusura percutanea del forame ovale dal 1 Febbraio 2016 al 30 Giugno 2024, dei quali verrà valutata l'incidenza di fibrillazione atriale sintomatica o asintomatica, quest'ultima mediante dispositivo esterno sopra cutaneo (Rooti Rx) o loop-recorder, valutati in modo consecutivo presso ambulatorio Heart and Brain coordinato congiuntamente dalle SOD Stroke Unit e Interventistica Cardiologica Strutturale dell'AOUC.* *Il periodo di osservazione del 1 Febbraio 2016 al 30 Giugno 2024.*
Indicare i soggetti interni che partecipano al trattamento quali persone espressamente designate o autorizzate[6] *N. 2 Direttori di Strutture Organizzative Dipartimentali (SOD Stroke Unit e Interventistica Cardiologica Strutturale)* *N. 2 Dirigenti Medici Strutturati di I Livello* *N. 2 Specializzandi* *N. 1 Statista*
Indicare eventuali soggetti esterni che partecipano al trattamento quali titolari, responsabili o persone designate/autorizzate al trattamento[7] *Nessuno*
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 trattati sono raccolti all'interno delle cartelle elettroniche ArchiMed e ArchiAmbu, così come nel registro ambulatoriale Heart and Brain istituito secondo protocollo aziendale. Da tali registri verranno estratti tutti i dati clinici dei pazienti afferenti*

all'ambulatorio preposto e sottoposti a chiusura percutanea del forame ovale e riscontro di fibrillazione atriale ad ECG o mediante monitorizzazione elettrocardiografica con dospositivi Rooti Rx e loop recorder. Successivamente verranno selezionati soltanto i dati di interesse scientifico in ottica di ricerca medica secondo le competenze dell'Heart and Brain Team. I dati selezionati verranno pseudonimizzati e quindi inseriti all'interno del database RedCap, in una CFR appositamente creata, il cui accesso sarà protetto da una password per l'apertura del file trasmessa separatamente. I dati raccolti verranno sottoposti ad analisi statistica per valutare l'incidenza delle alterazioni del ritmo cardiaco insorte dopo la chiusura del forame ovale e l'eventuale associazione con i diversi tipi di device utilizzati

Indicare dove vengono archiviati e conservati i dati[9]

I dati saranno archiviati sul sistema 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 (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: indicare i criteri utilizzati per garantire l'adeguatezza, la pertinenza e la non eccedenza dei dati utilizzati[12]

Verranno utilizzati soltanto i dati clinici indispensabili all'esecuzione dello studio.

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

Il termine di conservazione dei dati è fissato a 7 anni. Si evidenzia la consapevolezza che la valenza normativa dei termini di conservazione previsti dalle disposizioni vigenti, sempre orientate a regolare gli studi interventistici, non è direttamente ed immediatamente prescrittiva per gli studi osservazionali, così che viene comunque chiamata in causa la responsabilizzazione del Titolare. Si è considerato opportuno applicare a questo studio osservazionale il termine di conservazione di 7 anni già previsto dal D.Lgs. 200/07, riferibile ad una prassi consolidata e soprattutto ritenuta 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 all'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:

Gli utenti sono profilati e l'accesso al database RedCap e le operazioni svolte sono tracciate

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

La pseudonimizzazione dei dati avverrà attraverso l'assegnazione di un codice. 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.

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]

Non è previsto un sistema di crittografia.

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

Prima della pubblicazione i dati saranno anonimizzati, ricorrendo a tecniche di anonimizzazione, che consistono nel

generalizzare gli attributi delle persone interessate, diluendo i livelli di dettagli.

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

I Direttori di Strutture Organizzative Dipartimentali (SOD) avranno accesso alla sola lettura dei dati.
Il PI avrà accesso a tutte le informazioni raccolte e a tutte le operazioni (lettura, scrittura, cancellazione ed elaborazione).
I Medici Strutturati di I Livello ed i Medici in formazione Specialistica afferenti alla Stroke Unit avranno accesso alla lettura, scrittura, elaborazione, cancellazione dei dati clinici.
I Medici Strutturati di I Livello ed i Medici in formazione Specialistica afferenti alla Interventistica Cardiologia Strutturale avranno accesso alla lettura, scrittura, elaborazione, cancellazione dei dati cardiologici.
Lo Statistico avrà accesso alla lettura e alla elaborazione dei dati

Indicare se gli accessi sono tracciati[20]

Tutti gli accessi verranno tracciati dal sistema REDCap.

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

Il backup dei dati verrà effettuato ed assicurato una volta alla settimana

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

Il sistema prevede misure contro virus e malware installate nei PC aziendali.

Indicare se i dati sono trattati anche su supporti cartacei, e come questi sono gestiti[23]

E' prevista una archiviazione cartacea dei moduli di consenso al trattamento limitatamente ai pazienti contattabili. Responsabili dell'archiviazione è il e PI dello studio che conserveranno il materiale in un armadietto chiuso a chiave e al quale hanno accesso solo loro.

DIRITTI DEGLI INTERESSATI

Ove applicabile: indicare come sono informati gli interessati al trattamento[24]

Gli interessati saranno informati mediante la messa a disposizione dell'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[25]

Vista l'esiguità del personale strutturato e non strutturato (peraltro già impegnato nella attività clinica, raccolta dati, analisi ed interpretazione dei risultati), e l'elevato numero dei pazienti coinvolti, si ritiene che non sia possibile ricontattare tutti i partecipanti allo studio per la raccolta del consenso informato.
Si ritiene verosimile che parte dei pazienti, visti i tempi trascorsi dalla prima valutazione ambulatoriale, risultino non contattabili; il paziente sarà considerato non contattabile dopo 3 tentativi telefonici senza esito positivo.

Ove applicabile: indicare come è acquisito il consenso degli interessati[26]

Si potrà procedere alla acquisizione del consenso informato solo nel caso in cui i pazienti abbiano già un appuntamento fissato presso l'ambulatorio Heart and Brain

Ove applicabile: indicare se il trattamento coinvolge soggetti qualificati come responsabili del trattamento[27]

Non applicabile

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 veicolate 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 ridondanti 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)

Dr. Francesco Meucci

FIRMA	*Data 03/03/2025*