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

Denominazione del trattamento

"Studio osservazionale monocentrico retrospettivo su schede di registrazione delle chiamate telefoniche al Centro di Tossicologia Perinatale per esposizione farmaci antidepressivi in gravidanza. Prot. TOX PER 4

Finalità del trattamento

1. Obiettivo primario di questo studio è di valutare retrospettivamente il tasso di malformazioni maggiori nei neonati dopo esposizione materna a farmaci antidepressivi SSRI durante la gravidanza rispetto a quello di un gruppo di controllo di donne che hanno contattato il nostro centro in relazione all'esposizione a sertralina in gravidanza.
2. Obiettivo secondario dello studio è quello di quantificare il tasso di esiti avversi della gravidanza definiti come nati morti, aborti spontanei, interruzione volontaria o terapeutica della gravidanza, nati pretermine e nati piccoli per età gestazionale nei due gruppi.

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

Dati materni:

- Data della chiamata
- Data della ultima mestruazione
- Età
- Etnia
- BMI
- Precedenti ostetrici
- Familiarità per malformazioni congenite
- Anamnesi patologica materna
- Anamnesi farmacologica materna
- Assunzione di sostanze per uso voluttuario
- Complicanze avvenute in gravidanza
- Esito della gravidanza

Dati neonatali raccolti al follow-up telefonico effettuato tre mesi dopo la data presunta del parto:

- Data di nascita
- Sesso
- Settimana di gestazione alla nascita
- Peso, lunghezza e circonferenza cranica ed indici di Apgar alla nascita
- Patologie neonatali diagnosticate nei primi tre mesi di vita
- Malformazioni congenite diagnosticate nei primi tre mesi di vita

Dati paterni

- etnia

Il trattamento ricomprende l'utilizzo di strumenti di Intelligenza Artificiale? Se SI qual è la logica di funzionamento?

NO

Indicare le tipologie di interessati al trattamento[2]

Verranno presi in considerazione tutte le schede di registrazione riferite alle donne in gravidanza che hanno telefonato al centro di tossicologia perinatale per aver assunto paroxetina, duloxetina, venlafaxina vortioxetina che corrispondono ai criteri di inclusione/esclusione indicati nel periodo che va dal 01/01/2013 al 31/12 2024. Non è possibile determinare con precisione la numerosità campionaria delle schede di registrazione delle chiamate che saranno incluse nello studio ma si prevede di includerne almeno 500 nel gruppo di studio e almeno 1500 nel gruppo di controllo (donne che hanno assunto sertralina in gravidanza). Poiché si prevede si utilizzare come metodo di analisi predittiva la regressione logistica 500-1000 casi saranno sufficienti per stimare i parametri in oggetto.
.

Indicare i soggetti interni che partecipano al trattamento quali persone espressamente designate o autorizzate

Oltre al PI dello studio, Dott. Andrea Missanelli, un altro medico afferente alla SOD di Tossicologia Medica e Centro Antiveleni

Indicare eventuali soggetti esterni che partecipano al trattamento quali titolari, responsabili o persone designate/autorizzate al trattamento

Nessuno

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

Il macroflussodei dati sarà il seguente: Archimed (cartella clinica) >Redcap (CRF) > STATA (software statistica)
Verrà effettuata una estrazione di dati dalla cartella clinica elettronica aziendale Archimed, sulla base di item predefiniti, producendo cosi un foglio excel nel quale, saranno inserite alcune informazioni desunte dalla anamnesi e contemporaneamente sarà effettuato, da parte di un componente del gruppo di sperimentazione, un controllo sulla cartella clinica originale per verificare l'esattezza dei dati raccolti. Dal foglio excel saranno quindi eliminati i riferimenti anagrafici ed il numero di cartella clinica (numero nosologico) ed i dati saranno pseudonimizzati associando ad ogni paziente un codice alfanumerico registrato in un documento a parte, in esclusivo possesso dello sperimentatore principale.
Il foglio excel sarà a questo punto importato su una Case Report Form (CRF) adeguatamente strutturata su "REDCAP" e subito dopo cancellato.
Per consentire l'elaborazione statistica dei dati da "REDCAP" sarà nuovamente estratto un file excelche sarà trasferito immediatamente sul software di statistica installato sul server aziendale STATA (statistical software for data science).I dati aggregati generati da STATA saranno salvati in un file pdf ed a questo punto il file Excel verrà cancellato.

Indicare dove vengono archiviatie conservati i dati

I dati saranno archiviati e conservati sulla piattaforma web Redcap

PRINCIPI FONDAMENTALI[3]

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)[4]

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[5]**

I dati estratti dall'applicativo ARCHITOX sono solamente quelli indispensabili alla ricerca.

***Limitazione della conservazione*: indicare per quanto tempo sono conservati i dati e i criteri per la conservazione dei dati[6]**

I dati saranno conservati per 3 anni dalla pubblicazione dello studio.

***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[7]**

I dati estratti sono ricontrollati sulla cartella clinica originale dal gruppo di sperimentazione

***Integrità e riservatezza dei dati*[8]:** 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[9]

I dati saranno pseudonimizzati associando ad ogni paziente un codice alfanumerico registrato in un documento a parte, in esclusivo possesso dello sperimentatore principale.

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)[10]

Nessuna cifratura dei dati

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono anonimizzati, e secondo quali modalità[11]

I dati relativi ad ogni paziente saranno anonimizzati al momento della aggregazione dei dati (analisi file STATA)

Indicare i criteri di profilazione per l'accesso ai dati[12]

L' applicativo aziendale AOUC Architox è accessibile solo da PC interni alla Azienda e solo tramite username e password personali concessa solo dallo sperimentato principale e solo agli altri sperimentatori.
L'acceso a REDCAP e a STATA è possibile solo allo sperimentatore principale.

Indicare se gli accessi sono tracciati[13]

Gli accessi al PC sul quale sono conservati i dati sono tracciati. Gli accessi e le modifiche al eCRF "REDCAP" sono tracciati.

Indicare con quale frequenza viene effettuato il backup dei dati[14]

Il backup della cartella viene eseguito ogni 24 ore

Indicare se il sistema prevede misure contro virus e malware[15]

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[16]

Non è previsto un trattamento di dati effettuato su supporti cartacei

DIRITTI DEGLI INTERESSATI

Indicare come sono informati gli interessati al trattamento[17]

si ritiene di non potere informare gli interessati, in quanto il servizio erogato è solo di informazioni al telefono.

Indicare le ragioni per cui non è possibile informare gli interessati[18]

A nostro giudizio la acquisizione del consenso informato da tutte le pazienti arruolabili risulta impossibile o implica uno sforzo sproporzionato per i seguenti motivi:

- la natura retrospettica dello studio
- le particolari modalità di acquisizione dei dati sulla scheda di registrazione della chiamata telefonica tramite il solo contatto telefonico.
- la numerosità del campione richiesto per lo studio
- l'esiguo numero di sperimentatori coinvolti nella ricerca
- la oggettiva difficoltà a convocare le pazienti a Firenze da tutto il territorio nazionale per farle firmare il consenso informato
- il notevole intervallo di tempo trascorso dal momento della acquisizione dei dati al momento dell'inizio dello studio

La acquisizione del consenso informato da parte del padre biologico del neonato interessato dallo studio prevede inoltre alcune difficoltà aggiuntive:

- Il contatto telefonico avviene esclusivamente con la donna in gravidanza e nella scheda di registrazione non sono raccolti dati anagrafici o contatti del padre biologico del neonato; l'unico dato riguardante il padre è la sua appartenenza o meno alla etnia caucasica ed è raccolto dalla anamnesi della donna in gravidanza e non dal soggetto.
- Nei casi di procreazione medicalmente assistita, con fecondazione eterologa attraverso donazione dello sperma, l'identità del padre non è conosciuta.
- La donna potrebbe, in alcuni casi, non essere interessata ad informare il padre biologico del neonato della gravidanza pregressa.

La acquisizione del consenso informato da parte del neonato interessato dallo studio, diventato nel frattempo maggiorenne, risulta, per tutti i motivi sopraelencati, ancora più difficoltosa.

La mancata acquisizione del consenso informato da parte di una frazione anche ridotta dei soggetti arruolabili oltre a ridurre numericamente la dimensione dl campione introdurrebbe una sorta di "preselezione" nella metodica dello studio che inficerebbe la qualità scientifica dello studio.

Vorremmo quindi procedere secondo le modalità di cui all'art. 36 del Regolamento (art.110 del Codice in materia di protezione dei dati personali, art.9, par. 2, lett.j), ovvero mediante sottoposizione del protocollo di studio a consultazione preventiva da parte del Comitato Etico Area Vasta Centro

Indicare, per gli studi per i quali è possibile, come è acquisito il consenso di quota parte degli interessati[19]

Come sopra anticipato, si ritiene di non potere acquisire il consenso degli interessati

Indicare se il trattamento coinvolge soggetti qualificati come responsabili del trattamento[20]

N.A

GESTIONE DEI RISCHI[21]
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(vedi nota 1)
(nome/cognome)

Dr. Andrea Missanelli

FIRMA 	*Data 08/03/2026*

[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'interessato è la persona fisica cui si riferiscono i dati personali trattati: in uno studio, sono ad esempio i pazienti in esso arruolati, descritti attraverso le caratteristiche (es. di patologia, esiti, età) che li rendono in esso eleggibili.Occorre qui Indicare anche il range temporale entro il quale si vanno ad identificare i pazienti eleggibili allo studio (es. pazienti diabetici trattati dal 1995 al 2020).
[3]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)

[4]La base giuridica ordinaria del trattamento dei dati a scopo di ricerca clinica è il consenso degli interessati, a seguito di idonee informazioni. Il consenso non è necessario se l'interessato non è contattabile, o se sitrattadi studio previsto da una norma di legge/da una disposizione regolamentare/ dal diritto UE/dal programma di ricerca sanitaria di cui all'art. 12 bis del D.Lgs. 502/92.
Nel caso che non sia possibile informare l'interessato ed acquisirne il consenso, e si tratti di studio previsto da una norma di legge/da una disposizione regolamentare/ dal diritto UE/dal programma di ricerca sanitaria di cui all'art. 12 bis del D.Lgs. 502/92, occorre riportare quanto segue (scegliendo il caso d'interesse):

- La base giuridica del trattamento è rappresentata dalla legge (specificare), che ha previsto lo studio.
- La base giuridica del trattamento è rappresentata dalla disposizione regolamentare (specificare), che ha previsto lo studio.
- La base giuridica del trattamento è rappresentata dalla normativa UE
- La base giuridica del trattamento è rappresentata dal programma di ricerca sanitaria di cui all'art. 12 bis del D.Lgs. 502/92 (specificare l'anno), che ha previsto lo studio.

Se il paziente non è contattabile - perché i dati di contatto sono stati perduti o non sono aggiornati, oppure il paziente è deceduto, o è preferibile non informarlo per motivi etici (es. il paziente non è informato sulla patologia di cui è affetto) – oppure se i contatti non sono gestibili per oggettiva impossibilità di carattere organizzativo (contattare i pazienti comporterebbe un impegno sproporzionato rispetto alle risorse disponibili), la base giuridica del trattamento, è rappresentata dal parere positivo del comitato etico competente a livello territoriale, nonché dalla applicazione di misure di garanzia sulla sicurezza del trattamento (che qui stiamo appunto specificando).
[5] La minimizzazione dei dati si traduce appunto nella garanzia che i dati siano "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati", art. 5 paragrafo 1 c del Regolamento). Ovvio che tali requisiti non possano essereassolutizzabili, in quanto strettamentefunzionali allo scopo di un dato studio: sarà comunque lecito utilizzare, tanto da un punto di vista qualitativo che quantitativo, soltanto le informazioni indispensabili per quel determinato studio.Chi valuta quali dati sono o meno necessari? Ovviamente il Titolare (e per esso, in un progetto di ricerca, il P.I.) che, nell'ottica della responsabilizzazione, dovrà argomentare e sostenere tale valutazione.Nel nostro caso occorre dunque dimostrare che i dati trattati, e già sopra elencati, sono soltanto quelli necessari alla realizzazione dello studio, e non altri..E' di tale necessità– strettamente correlata alla razionalità dello studio da un punto di vista eminentemente scientifico - che deve essere data brevemente evidenza, anche soltanto indicando in sintesi che "i dati raccolti sono quelli indispensabili alla esecuzione dello studio". In relazione a certe tipologie particolari di informazioni, ad es. quelle relative alle origini razziali o alla appartenenza etnica, può essere opportuno offrire una motivazione più puntuale ed articolata.
[6]Un termine puntuale per la conservazione dei dati utilizzati per gli studi osservazionali non è previstoe dunque quello scelto deve essere motivato.Il termine deve essere commisurato allo scopo principale della conservazione dei dati, che è anzitutto quello di rendere possibili verifiche o controlli della base dati dello studio successivamente alla pubblicazione.Si consiglia di scrivere qualcosa di analogo a quanto segue:

Il termine di conservazione dei dati è fissato a … (inserire il numero di anni ritenuto necessario) anni; si evidenzia la consapevolezza chela valenza normativa dei termini di conservazione previsti dalle disposizioni vigenti, sempre orientate a regolare gli studi interventistici, nonè 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 … anni in quanto …

Se si utilizza il termine di prassi di 7 anni, la motivazione può essere resa come segue, sostituendo l'ultima frase:

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.

Si ricorda che mediante l'informativa ex art. 13 o ex art. 14 del Regolamento occorre indicare e comunicare ai soggetti interessati, che:

- sono raccolti solo i dati strettamente necessari per il perseguimento delle finalità;
- decorsi i termini di conservazione, i dati personali saranno distrutti, cancellati o resi anonimi (descrivendo i meccanismi per la cancellazione o anonimizzazione dei dati).

Se i dati sono conservati a tempo indeterminato a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è necessario indicarlo e motivarlo, anche in riferimento a specifiche prescrizioni normative.

[7]In questo caso l'esattezza del dato non si intende riferita al suo aggiornamento, ma alle modalità con le quali i dati sono raccoltidalla documentazione originale e dunque duplicati, garantendone appunto l'esattezza rispetto a quella, per le finalità dello studio. Ovvio che misure di controllo sono meno necessarie quando l'estrazione da un data base informatico avviene quasi automaticamente a seguito dell'inserimento di dati parametri, rispetto alla copia manuale, per la quale occorre individuare una procedura di verifica e controllo.

[8] Ai sensi dell'art. 5 par. 2 del Regolamento, i dati devono essere "trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)". Le politiche di sicurezza sono necessarie per evitare:

- la divulgazione di dati personali o l'accesso agli stessi non autorizzati o accidentali;
- la modifica non autorizzata o accidentale di dati personali (così che i dati sono modificati o incompleti);
- la perdita della possibilità di accesso o distruzione accidentale o non autorizzata di dati personali.

Occorre indicare, sinteticamente, le misure adottate da un punto di vista organizzativo, nonché quelleinformatiche assicurate dal sistema sul quale i dati sono archiviati, anche attraverso il rimando alla relativa documentazione tecnica.

E' ovvio che la modifica, la perdita o la non accessibilità ai dati sono questioni che non attengono esclusivamente alla privacy, ma direttamente alla qualità del dato di ricerca.

[9] La pseudonimizzazione(non *pseudo-anonimizzazione*, come si trova in qualche protocollo) consiste nell'associare dei dati (es. quelli relativi alla salute del partecipante allo studio) ad una informazione di carattere non identificativo (ad es. un codice), sostituendo con essa quella di carattere identificativo, ad es. il nome/cognome dell'interessato, e mantenendo riservata, con specifiche misure di sicurezza, la correzione tra dato identificativo e dato non identificativo (tra anagrafica e codice). Essa è una operazione di trattamento che si traduce in una misura di sicurezza e di minimizzazione dei dati. Non ogni codificazione può tradursi in unapseudonimizzazione dei dati: non lo è certo l'utilizzo del codice fiscale (ben più identificativo del mero nome giuridico), ma neppure un codice che sia conosciuto al di fuori del gruppo di sperimentazione (es. il numero nosologico o simile, anche a livello di singolo reparto).

Occorre descrivere come è costruito il codice, e come è strutturato e gestito il processo di pseudonimizzazione dei dati, cioè in quale fase dello studio si attua.

Comunque, se si crea un elenco, e questo ha una sua logica (ad es. alfabetica o cronologica), non è sufficiente togliere l'anagrafica ed inserire ad es. dei codici progressivi, occorre che siano non sequenziali e randomizzati (almeno se l'estrazione dei dati è eseguibile una seconda volta con identici risultati). Insomma, il codice di pseudonimizzazione non può contenere elementi oggettivi – informativi o di carattere procedurale – che rendano possibile una identificazione dell'interessato a prescindere dalla chiave di pseudonimizzazione.Si può scrivere quanto segue:

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.I codici di pseudonimizzazione sono costruiti secondo la seguente modalità: ……. I dati sono pseudonomizzati …. (*indicare in quale fase avvien la pseudonimizzazione dei dati*)

[10] Occorre precisare se i dati, in qualche momento del processo (es. trasferimento o comunicazione, oppure archiviazione, sono cifrati, e con quale tecnica.

[11] Si ricorda che, per anonimizzazione ci si riferisce ad una tecnica che si applica ai dati personali al fine di ottenere unaloro deidentificazione assoluta e irreversibile. In pratica, il dato anonimizzato non potrà più essere, in nessun contesto di trattamento, neppure in quello originario, ricollegato all'interessato. In pratica, un set di dati privato dell'anagrafica non è, come secondo la nozione etimologica o di senso comune, un dato anonimizzato: è, piuttosto, un dato personale non immediatamente

identificativo. Un set di dati è anonimizzato solo quando è definitivamente e irreversibilmente privato, anche prospetticamente, di una possibilità di raccordo con la relativa anagrafica, nel senso che questa non è più recuperabile (e non è dunque più possibile una reidentificazione, cioè la eventualità che, partendo da dati erroneamente ritenuti anonimi, si riesca a recuperare informazioni identificative degli interessati, sia direttamente, sia tramite metodi di correlazione e deduzione).
Con questi presupposti, il dato anonimo/anonimizzato ben raramente può essere presente in uno studio se non nella fase conclusiva, quando si aggregano i dati in vista della pubblicazione degli esiti. La procedura con cui si anonimizzano i dati in vista della pubblicazione deve essere descritta; ordinariamente, non essendo auspicabile, in uno studio clinico il ricorso a tecniche di *randomizzazione*, che consistono nella modifica della veridicità dei dati, si ricorrerà a tecniche di *generalizzazione*, consistono nel generalizzare gli attributi delle persone interessate, diluendo i livelli di dettaglio. Si utilizzerà di solito, tra queste, il K.-Anonimato, tecnica volta ad impedire l'individuazione di persone interessate mediante il loro raggruppamento con almeno K altre persone (K=valore di soglia). Secondo la regola della soglia, le persone cui si riferiscono i dati si considerano non identificabili se il loro numero è superiore ad un certo valore prestabilito (valore di soglia). Il valore minimo ordinariamente attribuibile alla soglia è pari a tre (ma nel valutare il valore della soglia si deve tenere conto del livello di sensibilità delle informazioni, e dell'effettivo rischio di danno ad esse correlato). La regola della soglia sottende che il valore originale X possa essere riferito non al solo Caio, ma anche a Tizio, Tazio e Sempronio. La relazione biunivoca tra il valore X ed una (una sola) persona fisica viene così meno. Occorre indicare come si procede quando una tipologia di informazione resta sotto la soglia minima.

[12] La profondità di accesso indica il *quantum* di accessibilità ai dati che è riconosciuto ad una determinata persona autorizzata al trattamento (cfr. nota 6); essa deve riguarda tanto la quantità e la tipologia di informazioni accessibili, che le operazioni (lettura, scrittura, cancellazione, elaborazione ecc.) eseguibili sui dati. Tutte queste prerogative sono connesse ad uno o più profili di autorizzazione (e, correlativamente e simmetricamente, di protezione dei dati), che si chiede – qualora plurali - di elencare e descrivere nei loro contenuti.

[13] Il tracciamento degli accessi, con finalità di sicurezza e controllo, può riguardare tanto operazioni che modificano la consistenza dei dati che la loro mera consultazione. Tale tracciamento si traduce nella conservazione,per un certo periodo di tempo, di file di log (il log file è appunto un file che contiene un elenco cronologico delle attività svolte da un sistema operativo, da un database o da altri sistemi, per permettere una verifica successiva). E' richiesto di specificare, appunto, se sono tracciati gli accessi degli utenti e degli amministratori, se sono tracciati anche gli accessi in consultazione, se sono tracciati i riferimenti temporali degli accessi, per quanto tempo gli eventuali file di log sono conservati. Il tracciamento degli accessi, con la registrazione delle operazioni effettuate, in particolare di modifica dei dati, è una misura essenziale per garantire la sicurezza dei dati, in particolare la loro esattezza ed integrità.
Per quanto riguarda la documentazione cartacea, si deve indicare se si procede o meno ad un controllo degli accessi fisici.

[14] Tra le misure che ostano alla perdita, totale o parziale, dei dati, vi è il backup, che può essere svolto con una diversa frequenza. Si chiede di precisare se il backup dei dati è assicurato, e con quale tempistica.

[15]Il termine malware indica un programma che è stato progettato per danneggiare un computer; è una sorta di genere ampio, rispetto alle specie quale troian , virus ecc.. Un virus è un malware che tende a danneggiare file e dati.

[16] La gestione dei supporti cartacei, in questo caso, riguarda la loro archiviazione sicura e la loro accessibilità. Si ricorda che, anche se il trattamento è solitamente effettuato con strumenti elettronici, laddove presente l'acquisizione del consenso è quasi sempre effettuata utilizzando supporti cartacei.

[17] La modalità ordinaria è la messa a disposizione dell'interessato dell'informativa redatta ai sensi dell'art, 13 del Regolamento.

[18]Qualora non sia possibile o opportuno informare gli interessati ed acquisirne il consenso occorre non solo attestarne ma documentarne e comprovarne i motivi tra i seguenti:

- ✓ motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione e l'informativa comporterebbe la rivelazione di notizie la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi;
- ✓ motivi di impossibilità organizzativa, nel senso che gli interessati, all'esito di ogni ragionevole sforzo compiuto per contattarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente) risultino essere al momento dell'arruolamento nello studio deceduti o comunque non contattabili, e 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 (avuto riguardo ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti).

Alcuni esempi:

- 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);

- irreperibilità e/o oggettiva impossibilità organizzativa dovuta all'elevato intervallo di tempo tra il primo accesso del paziente al centro (di sperimentazione coinvolto) ed il data entry dello Studio;
- impossibilità organizzativa e/o di fatto dovuta alla lontananza geografica dei pazienti che rende eccessivamente difficoltoso 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;
- intervenuta incapacità di intendere e/di volere dovuta all'aggravarsi dello stato clinico;
- sforzo oggettivamente sproporzionato rispetto agli obiettivi dello Studio che rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

Comunque, nel caso in cui informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, occorre documentare le valutazioni effettuate e le evidenze raccolte per sostenere ciò, anche con riferimento a dati statistici (ad es. circa la mortalità della patologia oggetto dello studio) e, se del caso, i tentativi di contatto effettuati ed i loro esiti percentuali sul totale dei pazienti arruolabili, oppure l'impegno di risorse materiali ed umane che, in riferimento al numero dei pazienti da contattare, rende l'operazione non sostenibile dal punto di vista organizzativo.
Occorre inoltre predisporre una informativa ex art. 14 del Regolamento, articolo che riguarda appunto le informazioni da mettere a disposizione dei pazienti non contattabili (nel caso dei defunti, dei loro aventi causa) come previsto dall'art. 6 delle *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica*… ; l'informativa sarà pubblicata in una sezione dedicata del sito istituzionale per tutta la durata dello studio stesso (nel caso di pazienti defunti, a beneficio di familiari ecc.).
Nell'informativa occorre indicare il soggetto cui sarà possibile rivolgersi, nel Centro di sperimentazione, per far valere i diritti degli interessati; si indica ordinariamente il responsabile aziendale della protezione dei dati, rpd@aou-careggi.toscana.it , 3666823917.

[19]Il «consenso al trattamento» è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile, con la quale l'interessato manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. Il consenso, in quanto "manifestazione di volontà", deve appunto manifestarsi, ed è dunque prestato mediante un atto positivo inequivocabile, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò può comprendere la selezione di un'apposita casella in un sito web o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non configura pertanto consenso il silenzio, l'inattività o la preselezione di caselle. Ad ogni modo, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.

[20]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.

[21] 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 ad 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.