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

M/903/150-C
Rev. 4

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. È 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] **"Epidemiologia delle otomastoiditi acute in età pediatrica: Studio osservazionale monocentrico retrospettivo e prospettico"**
Indicare la finalità del trattamento[3] *Il trattamento è funzionale alla conduzione di uno studio osservazionale il cui obiettivo principale è descrivere l'epidemiologia dei casi di otomastoidite acuta nella popolazione pediatrica.*
Indicare le tipologie di dati oggetto del trattamento, specificando ogni tipologia di dato[4] *Saranno trattati dati demografici e clinici registrati all'interno della cartella clinica.*
Indicare le tipologie di interessati al trattamento[5] *Bambini di eta' <14 anni affetti da otite media acuta (OMA) complicate da otomastoidite di cui non sono chiari l'epidemiologia come pure il percorso diagnostico-terapeutico e gli esiti.* *Lo studio sarà proposto consecutivamente ad ogni paziente e genitore e/o tutore di pazienti con diagnosi di otomastoidite acuta accertata (fase prospettica) che acceda al reparto SOC Pediatria e Neonatologia/TIN Santo Stefano. Anche i pazienti con diagnosi di otomastoidite acuta e accertata pregressa non più seguiti presso il reparto potranno essere inclusi nello studio previa acquisizione del consenso informato dei genitori/tutori (fase retrospettiva).*
Indicare i soggetti interni che partecipano al trattamento quali persone espressamente designate o autorizzate[6] *Personale medico afferente alla SOC Pediatria e Neonatologia/TIN Santo Stefano.*
Indicare eventuali soggetti esterni che partecipano al trattamento quali titolari, responsabili o persone designate/autorizzate al trattamento[7] *non previsti*
Descrivere il flusso dati (cioè come i dati sono spostati o elaborati). Occorre descrivere il flusso analiticamente nei suoi var

passaggi, operazioni, attori[8]

I dati demografici e clinici dei pazienti saranno estrapolati dalla cartella clinica elettronica (CR1; Argos).
La raccolta dei dati avverrà con l'ausilio della piattaforma web-based per la raccolta dati RedCap, fornita dal Promotore.
La piattaforma RedCap ha accesso limitato a soli utenti autorizzati tramite un sistema di autenticazione Utente/password, al fine di prevenire accessi non autorizzati.
Lo Sperimentatore Principale deve indicare i nominativi del personale delegato alla gestione dati, specificandone le relative funzioni nell'ambito dello studio nel Delegation log.
In fase di registrazione dei dati del paziente, la piattaforma RedCap prevede esclusivamente l'inserimento di un codice identificativo (ID) univoco associato all'anagrafica.
La lista di decodifica ossia quella lista che permette di collegare l'anagrafica del paziente al suo ID, sarà salvata e protetta all'interno di un file crittografato (con una password alfanumerica di almeno 14 caratteri), archiviata presso la SOC Pediatria e Neonatologia/TIN Santo Stefano e sotto la supervisione dello Sperimentatore Principale.

L'accesso alla piattaforma RedCap avviene tramite un PC Aziendale situato all'interno del reparto SOC Pediatria e Neonatologia/TIN Santo Stefano, il cui accesso è riservato al solo personale autorizzato.

I dati clinici richiesti dal protocollo verranno raccolti in forma pseudonimizzata dal personale designato dallo Sperimentatore Principale in una Scheda Raccolta Dati elettronica (eCRF) e gestita attraverso la piattaforma REDCap.

Indicare dove vengono archiviati e conservati i dati[9]

I dati relativi allo studio saranno archiviati dal Promotore in forma aggregata.

Le cartelle cliniche e la documentazione ambulatoriale con gli esami e gli aggiornamenti circa lo stato di salute del singolo caso restano archiviate su sistemi aziendali e con accesso limitato al solo personale autorizzato afferente alla SOC Pediatria e Neonatologia/TIN Santo Stefano.

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 degli interessati.
Per coloro che non sarà possibile informare e per i quali non sarà possibile ottenere il consenso, la base giuridica è rappresentata, dal parere positivo del competente comitato etico a livello territoriale (e la successiva autorizzazione del Direttore Generale dell'Azienda USL Toscana Centro), 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 personali sono adeguati, pertinenti e limitati giacché necessari ad avere un quadro clinico completo degli arruolati e, quindi, al raggiungimento della finalità dello studio.

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

I dati raccolti nel corso dello studio saranno registrati, elaborati, analizzati per tutta la durata del progetto, attualmente prevista per circa 5 anni e conservati unitamente al codice che identifica l'Interessato per 5 anni. Si precisa che soltanto lo Sperimentatore Principale ed i soggetti autorizzati del centro partecipante potranno collegare questo codice al nominativo mediante la lista di decodifica.

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]

I dati estrapolati e raccolti provengono da source documents originali (cartella clinica elettronica CR1 e Argos), verificati prima dell'inserimento nella eCRF di RedCap.

Integrità e riservatezza dei dati[15]: indicare le misure tecniche ed organizzative adottate per garantire la sicurezza dei dat

rispetto a trattamenti non autorizzati o illeciti, perdita, distruzione o danni accidentali, precisando quanto segue:

L'accesso alla piattaforma RedCap è vincolato al solo personale autorizzato dal Promotore, inserito nel Delegation log e afferente alla SOC Pediatria e Neonatologia/TIN Santo Stefano.

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

I dati clinici richiesti dal protocollo verranno raccolti in forma pseudonimizzata dal personale designato dallo Sperimentatore Principale nella eCRF della piattaforma REDCap.
La piattaforma RedCap prevede esclusivamente l'inserimento di un ID univoco associato all'anagrafica.
Verrà pertanto creata una lista di decodifica ossia la lista che permette di collegare il paziente al suo ID che sarà salvata e protetta all'interno di un file crittografato (con una password alfanumerica di almeno 14 caratteri), archiviata presso la SOC Pediatria e Neonatologia/TIN Santo Stefano, sotto la supervisione 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) [17]

per caratteristiche piattaforma RedCap, vedi DPIA del Promotore.

per quanto riguarda la lista di decodifica, questa sarà salvata e protetta all'interno di un file crittografato AES256 su PC Aziendale situato all'interno del reparto SOC Pediatria e Neonatologia/TIN Santo Stefano, il cui accesso è riservato al solo personale autorizzato.

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

I dati saranno resi anonimi prima della pubblicazione.

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

L'accesso alla piattaforma RedCap è limitato al personale autorizzato mediante un sistema di autenticazione Utente/password personale, al fine di prevenire accessi non autorizzati.

Indicare se gli accessi sono tracciati[20]

La piattaforma RedCap prevede controllo e tracciatura degli accessi. Per caratteristiche piattaforma RedCap, vedi DPIA del Promotore.

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

per caratteristiche piattaforma RedCap, vedi DPIA del Promotore.

per quanto riguarda la lista di decodifica, Il backup dei dati viene effettuato regolarmente, come previsto per le cartelle salvate su server aziendale (settimanalmente).

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

Tutti i PC aziendali sono aggiornati e dotati di efficaci software antivirus aggiornati e volti a contrastare eventuali malware.

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

Non è previsto l'utilizzo di supporti cartacei, fatto salvo i moduli di informativa e consenso dei pazienti risultati contattabili.

Questi saranno conservati presso la SOC Pediatria e Neonatologia/TIN Santo Stefano all'interno dell'Investigator Site File, in una stanza con accesso limitato e sotto la responsabilità dello Sperimentatore Principale

DIRITTI DEGLI INTERESSATI

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

Ai genitori/tutori del minore l'informativa, ai sensi dell'art. 13 del GDPR, viene fornita durante l'incontro di presentazione dello studio durante una visita di controllo, e in tale occasione viene raccolto il consenso specifico al trattamento dei dati.

Ove applicabile: indicare le ragioni per cui non è possibile informare gli interessati[25]

Per la coorte retrospettiva, esiste la possibilità che all'esito di ogni ragionevole sforzo compiuto dal personale medico per contattarli (verifica dello stato in vita, consultazione dei dati riportati nella documentazione clinica, l'impiego di recapiti telefonici eventualmente forniti nonché acquisizione dei dati di contatto pubblicamente accessibili), i pazienti risultino al momento dell'arruolamento, deceduti o non contattabili. In questa particolare evenienza il Garante riconosce il "motivo di impossibilità organizzativa" così come richiamato nelle "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice - 9 maggio 2024, pubblicate in G.U_Serie Generale n. 130 del 5 giugno 2024.
La mancata considerazione dei dati riferiti a questi, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe difatti conseguenze significative per lo studio in termini di alterazione dei relativi risultati.
In questo caso si prevede inoltre di rendere disponibili per tutta la durata dello studio le informazioni redatte ai sensi all'art. 14 del Regolamento UE 2016/679, mediante pubblicazione sul sito istituzionale dell Azienda USL Toscana Centro.

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

Nel caso in cui il paziente risulti contattabile, l'informativa ed il consenso informato verranno proposti al paziente durante una visita di controllo, e in tale occasione viene raccolto il consenso specifico al trattamento dei dati

Ove applicabile: 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; le password sono in possesso del solo personale interno autorizzato.

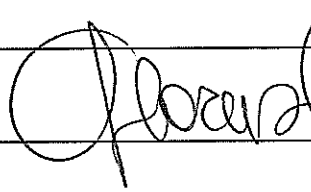
MODIFICHE INDESIDERATE DEI DATI

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 e l'accesso alla eCRF di RedCap è riservato al personale autorizzato della SOC Oculistica Prato, in possesso di password di accesso personali.

PERDITA DEI DATI

La probabilità di perdita dei dati è estremamente bassa visti i backup previsti dal sistema.

IL PREPOSTO AL TRATTAMENTO (vedi nota 1)
(nome/cognome)

FIRMA 	*Data* 22/4/2025

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 Inserire titolo e codice dello studio.
3 Finalità del trattamento vale il suo scopo pratico. Occorre dunque indicare, posto che il trattamento è ovviamente funzionale alla esecuzione dello studio, oltre allo scopo di ricerca in senso lato (es. "I dati sono trattati per scopo di ricerca in campo medico ..."), quali sono gli scopi che si intendono raggiungere con lo studio medesimo (es. scopo dello studio è verificare ..."). Qualora i dati vengano raccolti per una finalità ulteriore (es. di cura, il che significa che saranno trattati anche con modalità identificativa), occorre integrare tale specifico elemento nell'informativa sul trattamento dei dati.
4 In via generale si tratta di dati afferenti alle categorie particolari, es. relativi alla salute o genetici, e di dati comuni (es. dati anagrafici e di contatto). Oltre a questa indicazione più generica, categorica, occorre esplicitare i dati che vengono effettivamente raccolti; ciò può essere fatto con un grado maggiore (es. esiti di questo o quell'esame di laboratorio) o minore (es. esiti esami di laboratorio) di analiticità: è comunque preferibile essere più analitici possibile –questi elementi più puntuali sono normalmente già elencati nel protocollo - anche per motivare, se necessario, tali scelte in una prospettiva di minimizzazione (cfr. nota 12), cioè di una loro stretta funzionalità/indispensabilità rispetto allo studio.
5 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).
6 E' sufficiente indicare il numero dei componenti del gruppo di sperimentazione e le relative professionalità, senza indicazioni nominative. Per la persona espressamente designata, cfr. nota 1. La persona autorizzata al trattamento è la persona fisica – dipendente o collaboratore - sottoposta, per quanto concerne il trattamento dei dati, al Titolare (cioè l'Azienda), e che tratta dati personali solo nella misura in cui sia stata a ciò autorizzata e istruita: le istruzioni delimitano l'ambito di trattamento autorizzato, e precisano le modalità secondo le quali il trattamento deve essere effettuato. Nessun incaricato può trattare dati senza adeguate istruzioni (che sono un suo diritto), e nessun incaricato, ricevutele, può effettuare operazioni di trattamento ulteriori rispetto a quelle da esse consentite. Tali istruzioni, nell'ottica della responsabilizzazione del titolare (che consiste nell'applicare i principi previsti all'art. 5 del regolamento UE 2016/679, documentandone le modalità di applicazione), devono essere raccolte in un atto di nomina a firma del P.I. (atto che potrà essere anche riferito al gruppo di sperimentazione nel suo complesso, oppure, qualora i compiti, all'interno del gruppo di sperimentazione siano significativamente differenziati, essere più personalizzato e quindi nominativo).
7 Qui si può far riferimento:

- ad altri Centri di sperimentazione, che partecipano allo studio quali titolari autonomi o contitolari del trattamento (il Titolare del trattamento è il soggetto che, individuato una finalità, cioè uno scopo pratico, determina le modalità di trattamento dei dati necessarie per raggiungerlo; qualora finalità e modalità siano condivise, si può stabilire una condizione di contitolarità, che deve essere formalizzata mediante un accordo redatto ai sensi dell'art. 26 del Regolamento);
- a soggetti (normalmente enti) che collaborano funzionalmente allo studio (es. un laboratorio esterno che effettui esami previsti dalla ricerca) ma che non assumono il ruolo di titolare del trattamento in quanto non hanno partecipato alla definizione delle finalità e modalità del trattamento – cioè alla elaborazione e condivisione del protocollo di ricerca - e che quindi devono formalmente individuarsi come Responsabili del trattamento (vedi nota 27).

Occorre elencare tali soggetti deve, in riferimento allo stato attuale dello studio (in alcuni studi multicentrici, ulteriori partecipanti possono aderire al progetto successivamente) con la loro esatta denominazione.
8 Un trattamento di dati personali si traduce in un flusso di informazioni, che può coinvolgere vari spazi (es. banche dati), soggetti ecc., e che può sostanziarsi in una serie di operazioni (es. la raccolta dei dati, per la quale occorre indicare come essi vengono selezionati e archiviati, ad es. in un foglio di raccolta o in un database; o la loro comunicazione, tra due o più titolari; le modalità di elaborazione ecc.). E' necessario indicare anche se i dati sono meramente trasferiti all'interno di uno stesso ambito di titolarità: il trasferimento del dato è nozione più ampia, e talvolta diversa, da quella della sua comunicazione, cioè della trasmissione del dato ad altro titolare; questa comporta spesso un trasferimento di dati (ma i dati possono essere comunicati anche mettendoli semplicemente a disposizione, senza trasmetterli); si ha trasferimento di dati

sia se i dati sono trasferiti al di fuori dei sistemi aziendali, sia se sono meramente spostati anche all'interno del medesimo ambito di titolarità (cioè ad es. da un server all'altro dell'Azienda, o verso un server di un soggetto che agisce per il titolare, quale responsabile del trattamento). Occorre precisare se i dati sono eventualmente trasferiti:

- nell'ambito dell'Azienda
- fuori dall'Azienda
- fuori dall'Italia
- fuori dall'Unione Europea

Il trasferimento del dato, soprattutto se effettuato al di fuori del proprio ambito di titolarità (che normalmente corrisponde ad un perimetro presidiato), può rappresentare un momento critico, che necessita l'adozione di idonee misure di sicurezza tanto tecniche che organizzative: di quelle appunto specificamente riferibili al trasferimento del dato si richiede una breve descrizione. Il trasferimento dei dati (esclusi i dati genetici) deve essere effettato con modalità sicura, anche con strumenti di cooperazione applicativa oppure utilizzando strumenti di messaggistica che utilizzino canali di comunicazione protetti (ivi compresa la PEC), oppure, se si utilizzano sistemi di posta elettronica ordinaria, proteggendo l'allegato con tecniche di cifratura e rendendolo accessibile tramite una password per l'apertura del file trasmessa separatamente; qualora lo studio ricomprenda dati genetici, non sarà possibile utilizzare la mail ordinaria ma solo strumenti di cooperazione applicativa o di messaggistica che utilizzino canali di comunicazione protetti (ivi compresa la PEC), cifrando i dati e fornendo la chiave di decifrazione attraverso canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati. E' necessario richiamare eventuali agreement redatti per il trasferimento dei dati, e comunque documentare la valutazione della necessità e proporzionalità del trattamento che è stata effettuata.

9 Si distingue qui tra archiviazione e conservazione, indicando con la prima voce la temporanea allocazione dei dati nel corso dello studio, con l'altra quella effettuata nel periodo successivo al termine dello studio, prima della definitiva cancellazione o anonimizzazione dei dati (sono comunque operazioni che possono essere effettuate con continuità sul medesimo sistema), E' necessario individuare specificamente dove i dati vengono allocati, indicando anche il sistema o il data base utilizzato. Se per la loro successiva conservazione si utilizza, appunto, una banca dati diversa, occorrerà indicarla.

In ordine ai profili di sicurezza, anche in relazione alla esattezza ed integrità dei dati, è inutile precisare che un foglio excel su un pc in locale non soddisfa i requisiti minimi (la DPIA non otterrà il parere positivo del Responsabile della Protezione dei dati aziendale, e quand'anche venisse trasmessa, è certo che non sarà possibile ottenere la autorizzazione del Garante).

Il sistema di archiviazione e conservazione dei dati di studio messo a disposizione dall'Azienda è RedCap; possono essere utilizzati strumenti diversi, ma che garantiscano, allo stesso modo, un tracciamento degli accessi e delle operazioni effettuate e garanzie contro virus, malware ecc..

Qualora venga utilizzata una piattaforma esterna, occorrerà procurarsi le relative informazioni tecnico informatiche, da mettere agli atti della documentazione di studio (di tale documentazione si potrà offrire evidenza, allegandola o meno, nel presente documento); non è necessario che tale documentazione sia esaustiva da un punto di vista tecnico, ma deve essere tale da fornire informazioni sufficienti ad effettuare una minima valutazione di adeguatezza, anche con il supporto della componente tecnico-informatica aziendale.

10 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)

11 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 si tratta 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.

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).

12 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 essere assolutizzabili, in quanto strettamente funzionali 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.

13 Un termine puntuale per la conservazione dei dati utilizzati per gli studi osservazionali non è previsto e 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 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 ... 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.

14 In questo caso l'esattezza del dato non si intende riferita al suo aggiornamento, ma alle modalità con le quali i dati sono raccolti dalla 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.

15 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 quelle informatiche 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.

16 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 una pseudonimizzazione 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*)

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

18 Si ricorda che, per anonimizzazione ci si riferisce ad una tecnica che si applica ai dati personali al fine di ottenere una loro 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.

19 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.

20 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.

21 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.

22 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.

23 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.

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

25 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, responsabileprotezionedati@uslcentro.toscana.it,.

26 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.

27 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.

28 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 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 AUSL TC. 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.