



La DPIA (Data Protection Impact Assessment) – o anche VIP (Valutazione d'Impatto Privacy) - è un processo, che si risolve in un documento, inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Essa mette dunque a disposizione:

- una descrizione sistematica del trattamento;
- la esplicitazione delle finalità del trattamento;
- una valutazione della necessità e proporzionalità del trattamento;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure tecniche e organizzative che il titolare ritiene di dover adottare allo scopo di mitigare tali rischi.

La DPIA è redatta dal preposto al trattamento¹ e oggetto di valutazione del Responsabile della protezione dei dati.

DESCRIZIONE DEL TRATTAMENTO DEI DATI

Denominazione del trattamento²

TITOLO: L'effetto Macklin: un indicatore di barotrauma nei pazienti con Sindrome Da Distress Respiratorio Acuto (23650_PF)

Indicare la finalità del trattamento³

Gli obiettivi primari dello studio sono i seguenti:

- a) stimare l'incidenza dell'effetto Macklin nei pazienti con ARDS (Sindrome Da Distress Respiratorio Acuto) non COVID-19
- b) valutare l'associazione tra effetto Macklin e barotrauma nei pazienti con ARDS non COVID mediante la stima dell'incidenza del barotrauma nei pazienti con effetto Macklin rispetto ai soggetti nei quali l'effetto Macklin non è documentabile
- c) confrontare la mortalità intraospedaliera tra i pazienti che presentano effetto Macklin e quelli che non lo presentano

Obiettivi secondari dello studio:

- a) confronto tra l'incidenza di effetto Macklin tra i pazienti con ARDS non COVID e quello con ARDS COVID correlato
- b) stima dell'associazione tra barotrauma e effetto Macklin nei pazienti con ARDS COVID e confronto con quella nei pazienti con ARDS non COVID.

Indicare le tipologie di dati oggetto del trattamento, specificando ogni tipologia di dato⁴

DATI COMUNI data di nascita

DATI CLINICI peso altezza durata degenza mortalità, esiti di esami di laboratorio clinico e microbiologici esami Tc



Indicare le tipologie di interessati al trattamento⁵

Pazienti con grave insufficienza respiratoria acuta ricoverati presso la Terapia Intensiva “ Cure Intensive del trauma e Gravi Insufficienze d’Organo” tra il Gennaio 2018 e novembre 2022.

Indicare i soggetti interni che partecipano al trattamento quali persone espressamente designate o autorizzate e se queste siano state adeguatamente istruite sul trattamento⁶

Il gruppo di Sperimentatori è costituito da quattro ANESTESISTI RIANIMATORI e due RADIOLOGICI adeguatamente istruiti sul trattamento e le misure tese a garantire una adeguata protezione dei dati personali

Indicare eventuali soggetti esterni che partecipano al trattamento quali titolari, responsabili o persone designate/autorizzate al trattamento e se questi siano state adeguatamente istruiti sul trattamento⁷

Nessun soggetto esterno partecipa al trattamento

Descrivere il flusso dati (cioè come i dati sono spostati o elaborati). Occorre descrivere il flusso analiticamente nei suoi vari passaggi, operazioni, attori⁸

Dopo aver creato la struttura della CRF nel database Redcap, si procede ad estrarre dalla cartella clinica informatizzata aziendale Archimed un foglio excel recante le tipologie di dati d’interesse, coerenti con la struttura della CRF; si aggiungono al foglio Excell i dati radiologici, con doppio controllo di ogni singolo dato inserito. I dati archiviati sul foglio Excell sono pseudonimizzati ed il foglio viene importato, tramite una funzione nel database Redcap, nella CRF. Il file Excell viene cancellato, avendo avuto in questa fase unicamente la funzione di mezzo di trasferimento dei dati. Da Redcap viene poi estratto un foglio Excell sul quale vengono effettuate delle analisi (le elaborazioni sono cioè direttamente effettuate mediante il foglio di calcolo); una volta ottenuti i risultati, anche questo foglio Excell viene distrutto, così che l’unica base dati conservata sia quella su Redcap.

Indicare dove vengono archiviati e conservati i dati⁹

I dati vengono archiviati e conservati su Redcap, il database messo a disposizione dall’Azienda per la conduzione degli studi osservazionali.

Indicare se i dati sono trasferiti (si/no) ed eventualmente dove¹⁰

Redcap è stato recentemente spostato, dai server aziendali, nella infrastruttura regionale TIX

PRINCIPI FONDAMENTALI

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, per gli interessati che sarà possibile contattare è il consenso degli interessati, per quelli che non sarà possibile informare e per i quali non sarà possibile ottenere il consenso, è rappresentata, oltre che dal parere positivo del competente comitato etico a livello territoriale, dalla consultazione preventiva presso l’Autorità Garante per la protezione dei dati personali di cui all’art. 110 comma 1 secondo periodo del D.Lgs. 30 giugno 2003 n. 196 Codice in materia di protezione dei dati personali.



Minimizzazione dei dati: indicare i criteri utilizzati per garantire l'adeguatezza, la pertinenza e la non eccedenza dei dati utilizzati¹²

I dati raccolti, sopra elencati, sono soltanto quelli indispensabili alla realizzazione dello studio.

Limitazione della conservazione: indicare per quanto tempo sono conservati i dati e i criteri per la conservazione dei dati¹³

Il termine di conservazione dei dati è fissato a 3 (tre) anni. Si è considerato opportuno applicare a questo studio osservazionale tale termine di conservazione in quanto coerente con le politiche di verifica e pubblicazione della rivista sulla quale si prevede di pubblicare gli esiti 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 trattati¹⁴

L'esattezza dei dati deriva dal fatto che sono estratti automaticamente dalla cartella informatizzata Archimed e, relativamente ai dati radiologici, inseriti manualmente sul foglio Excell estratto da Archimed, dal fatto che viene effettuato un doppio controllo sulla documentazione originale.

Integrità e riservatezza dei dati: indicare le misure tecniche ed organizzative adottate per garantire la sicurezza dei dati rispetto a trattamenti non autorizzati o illeciti, perdita, distruzione o danni accidentali¹⁵

La sicurezza dei dati è garantita dal fatto che sono conservati in un sistema il cui accesso è subordinato all'utilizzo di credenziali personali e tutti gli accessi e le operazioni effettuate sono tracciati

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono pseudonimizzati, e secondo quali modalità¹⁶

Viene effettuata una pseudonimizzazione randomizzata dei dati prima del loro inserimento in Redcap. I dati identificativi vengono codificati con codice numerico. Le informazioni aggiuntive che sono necessarie per l'identificazione vengono conservate separatamente e soggette a misure protettive (password di accesso) gestite esclusivamente dal Promotore.

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono crittografati, e secondo quali modalità (ovvero quale sistema di crittografia è utilizzato)¹⁷

I dati non sono crittografati

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono anonimizzati, e secondo quali modalità¹⁸

Gli esiti della elaborazione sul foglio Excell rappresentano dati aggregati.

Indicare se i dati sono soggetti a partizione¹⁹

I dati non saranno soggetti a partizione

Indicare con quali misure e cautele viene effettuato il trasferimento dei dati²⁰

I dati non verranno trasferiti se non nel database Redcap

Indicare i criteri di profilazione per l'accesso ai dati²¹

Saranno profilati per l'accesso ai dati in lettura i componenti del gruppo di lavoro



Indicare se gli accessi sono tracciati²²

Il database Redcap traccia accessi ed operazioni effettuate

Indicare con quale frequenza viene effettuato il backup dei dati ed il sistema utilizzato²³

Il backup dei server viene effettuato periodicamente

Indicare se il sistema prevede misure contro virus e malware²⁴

Il server all'interno del quale sono archiviati i dati prevede misure contro virus e malware

Indicare se i dati sono trattati anche su supporti cartacei, e come questi sono gestiti²⁵

I dati non sono trattati da supporti cartacei

DIRITTI DEGLI INTERESSATI

Indicare come sono informati gli interessati al trattamento oppure, in alternativa, le ragioni per cui non è possibile informare gli interessati, specificando i dati di contatto del soggetto al quale gli interessati (o altri soggetti legittimati) possono indirizzare le proprie richieste relative all'esercizio dei diritti di accesso e di portabilità dei dati, dei diritti di rettifica e di cancellazione, dei diritti di limitazione e di opposizione²⁶

Gli interessati non possono essere informati per le seguenti ragioni:

Una significativa percentuale dei pazienti è deceduto (55%)

Sedoanalgesia per motivi terapeutici (non erano cioè coscienti durante il ricovero). Possono essere eventualmente ricontattati dopo le dimissioni. I tentativi di contatto saranno documentati. Dopo tre contatti inefficaci, il paziente sarà considerato "non contattabile".

Possono essere eventualmente ricontattati dopo le dimissioni. I tentativi di contatto saranno documentati. Dopo tre contatti inefficaci, il paziente sarà considerato "non contattabile".

Ove applicabile: indicare se gli obblighi del responsabile del trattamento sono chiaramente definiti e formalizzati, e in caso di risposta positiva precisare come²⁷

Non applicabile

Valutare se, in caso di trasferimento dei dati al di fuori della UE, i dati godono di una protezione equivalente²⁸

I dati non saranno trasferiti fuori da UE

GESTIONE DEI RISCHI²⁹

ACCESSO ILLEGITTIMO AI DATI



Indicare, anche alla luce delle misure pianificate, una stima della probabilità e gravità del rischio (indefinita, trascurabile, limitata, importante, massima) connesso alla perdita di riservatezza dei dati, specificando, se possibile, le principali minacce che potrebbero concretizzare il rischio e le principali fonti di rischio, 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

Indicare, anche alla luce delle misure pianificate, una stima della probabilità e gravità del rischio (indefinita, trascurabile, limitata, importante, massima) connesso alla perdita di integrità dei dati, specificando, se possibile, le principali minacce che potrebbero concretizzare il rischio e le principali fonti di rischio.

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

Indicare, anche alla luce delle misure pianificate, una stima della probabilità e gravità del rischio (indefinita, trascurabile, limitata, importante, massima) connesso alla perdita di disponibilità dei dati, specificando, se possibile, le principali minacce che potrebbero concretizzare il rischio e le principali fonti di rischio.

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)

FIRMA

Data



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 e 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 sovrintende 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, quali sono gli scopi che si intendono raggiungere con lo studio medesimo. 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, ad es. relativi alla salute o genetici, e di dati comuni (es. dati anagrafici e di contatto). Oltre a questa indicazione più generica, 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 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.

⁶ E' sufficiente indicare le professionalità afferenti al gruppo di sperimentazione.

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. 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 poi essere tale che il responsabile tratti i dati personali soltanto su istruzione documentata del titolare del trattamento.

L'indicazione di tali soggetti deve, nella misura del possibile, ricomprendere la loro 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 trasmessi, ad es. in un foglio di raccolta o in un database; il trasferimento dei dati – il loro mero spostamento, anche all'interno di un singolo titolare – o la loro comunicazione, tra due o più titolari; le modalità di elaborazione ecc.).



Una valutazione d'impatto - come eminente espressione della responsabilizzazione del titolare - si fonda anzitutto su un trattamento chiaramente e analiticamente conosciuto e descritto in ogni suo aspetto: la qual cosa, tra l'altro, assume anche una valenza organizzativa, con positiva ricaduta sul piano operativo e logistico dello studio.

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 Si precisa nuovamente (cfr. nota 8) che il trasferimento del dato non coincide con la sua comunicazione, cioè con la trasmissione ad altro titolare, e neppure con l'invio di informazioni al di fuori dei sistemi aziendali, ma con il suo mero spostamento anche all'interno del medesimo ambito di titolarità (cioè ad es. da un server all'altro dell'Azienda).

Occorre indicare inoltre se i dati sono eventualmente trasferiti:

- fuori dall'Azienda
- fuori dall'Italia
- fuori dall'Unione Europea

Il trasferimento dei dati (esclusi i dati genetici) deve essere effettuato 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.

In caso di trasferimento in uno stato Extra UE occorre valutare le condizioni che consentono il trasferimento (cioè il livello di protezione offerto dal Paese o dall'organizzazione presso i quali sono trasferiti e se sono state fornite adeguate garanzie ex art. 46 o se vi sono deroghe ex art 49 del Regolamento UE 2016/679).

¹¹ Nel caso che non sia possibile informare l'interessato ed acquisirne il consenso, e non 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:

La base giuridica del trattamento, per gli interessati che non sarà possibile informare e per i quali non sarà possibile ottenere il consenso, è rappresentata, oltre che dal parere positivo del competente comitato etico a livello territoriale, dalla consultazione preventiva presso l'Autorità Garante per la protezione dei dati personali di cui all'art. 110 comma 1 secondo periodo del D.Lgs. 30 giugno 2003 n. 196 Codice in materia di protezione dei dati personali.

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.

Si ricorda che, 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, nel Protocollo,



le valutazioni effettuate 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.

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, e sarà dunque 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, 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 indispensabili alla realizzazione dello studio. Tale necessità, normalmente, si evince dal protocollo di ricerca (che è peraltro trasmesso al Garante), laddove si elencano appunto le informazioni che si ritiene necessario raccogliere per raggiungere gli obiettivi dello studio. 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”.

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 possibile 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, per gli studi osservazionali, la valenza normativa dei termini di conservazione previsti dalle disposizioni vigenti, sempre orientate a regolare gli studi interventistici, è, se non assente, comunque non direttamente ed immediatamente prescrittiva, 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 indicare le misure adottate per garantire il principio di minimizzazione.

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 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 codice ed anagrafica). 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.

Si può scrivere quanto segue, precisando la fase in cui avviene la assegnazione dei codici e come essi sono costruiti:

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.

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. Si ribadisce che 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.

¹⁹ Per partizione dei dati si intende la loro separazione fisica in archivi dati distinti.

²⁰ Il trasferimento del dato (cfr. note 8 e 10), 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.

²¹ La profondità di accesso indica il *quantum* di accessibilità ai dati - tanto da un punto di vista quantitativo che di tipologia di informazioni - è concesso ad una determinata persona autorizzata al trattamento (cfr. nota 6); a questa possono inoltre essere riconosciute particolari possibilità di intervento sui dati (lettura, scrittura, cancellazione, elaborazione ecc.). 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 descrivere in breve.

²² 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 di file di log, che sono conservati per un certo tempo. 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, pare essere una misura essenziale per garantire la sicurezza dei dati, ovvero la loro esattezza ed integrità.

Per quanto riguarda la documentazione cartacea, indicare se si procede o meno ad un controllo degli accessi fisici.

²³ Tra le misure che ostano alla perdita, totale o parziale, dei dati, vi è senz'altro 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.

²⁴ Il termine malware indica un programma che è stato progettato per danneggiare un computer; è una sorta di genere ampio, rispetto alle specie quale trojan, virus ecc.. Un virus è un malware che tende a danneggiare file e dati.

²⁵ La gestione dei supporti cartacei, in questo caso, riguarda la loro archiviazione sicura e la loro accessibilità.



²⁶ Occorre predisporre per lo studio l'informativa ex art. 13 del Regolamento, da utilizzarsi quando gli interessati sono contattabili. Qualora non lo siano (anche perché defunti), occorre predisporre una informativa ai sensi dell'art. 14 del Regolamento, che, nel rispetto dell'art. 6 delle *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica* ... sarà resa disponibile mediante pubblicazione sul sito istituzionale del Centro di sperimentazione per la durata dello studio stesso (nel caso di pazienti defunti, a beneficio di familiari ecc.).

Nell'informativa è richiesto di indicare il soggetto cui sarà possibile rivolgersi, nel Centro di sperimentazione, per far valere i diritti; si indica ordinariamente il responsabile aziendale della protezione dei dati, rpd@aou-careggi.toscana.it, 3666823917.

²⁷ Per il Responsabile del trattamento cfr. nota 7.

²⁸ Si pone qui la nuovamente questione del trasferimento dei dati extra UE (cfr. nota 20), in paesi nei quali non vigono le stesse regole poste a tutela del diritto alla protezione dei dati personali dalla normativa europea; si chiede in particolare se sono stati redatti agreement per il trasferimento dei dati, documentando comunque la valutazione della necessità e proporzionalità del trattamento che è stata effettuata.

²⁹ Qualora si utilizzi RedCap, si può scrivere 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.