La DPIA (Data Protection Impact Assestment) – 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 trattamento[1] e oggetto di valutazione del Responsabile della protezione dei dati.

DESCRIZIONE DEL TRATTAMENTO
Denominazione del trattamento[2] Validazione di una nuova metodologia assistenziale da utilizzare nei nuclei Alzheimer.
Indicare la finalità del trattamento[3] Lo scopo del trattamento è quello di dimostrare che attraverso una specifica metodologia assistenziale è possibile gestire i gravi disturbi del comportamento in soggetti affetti da demenza, riducendo la contenzione farmacologica e recuperando alcune abilità funzionali residue.
Indicare le tipologie di dati oggetto del trattamento, specificando ogni tipologia di dato[4] Le informazioni che verranno raccolte sono relative: all'età del paziente, al sesso, alla sua diagnosi di ingresso nel nucleo Alzheimer, alla presenza di disturbi del comportamento all'ingresso e alla dimissione dal nucleo, ai risultati ottenuti con le scale di valutazione effettuate durante il ricovero nel nucleo; alla terapia farmacologica all'ingresso e alla dimissione
Indicare le tipologie di interessati al trattamento[5] Pazienti affetti da demenza e gravi disturbi del comportamento ricoverati nel nucleo Alzheimer della RSA Villa Serena di Montaione negli ultimi dieci anni.
Indicare i soggetti interni che partecipano al trattamento quali persone espressamente designate o autorizzate e se queste siano state adeguatamente istruite sul trattamento[6] L'estrazione, il trasferimento e l'elaborazione dei dati viene effettuata da una unica persona, individuata dai due titolari, per gli ambiti di titolarità di competenza, quali persona autorizzata al trattamento.
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 trattamento[7] La RSA Villa Serena di Montaione, oltre al Promotore Azienda Ospedaliero-Universitaria Careggi, sono individuate quali autonomi titolari del trattamento.

Descrivere il flusso dati (cioè come i dati sono spostati o elaborati). Occorre descrivere il flusso analiticamente nei suoi vari passaggi, operazioni, attori[8]

La RSA Villa Serena utilizza dal 2004 una cartella clinica elettronica denominata Cartella Utente Web. Il programma è in grado di estrapolare i dati d'interesse su un foglio Excel, il file viene salvato direttamente sul File Server di Villa Serena in una cartella nominativa che necessita, per l'accesso, di credenziali personali; le credenziali d'accesso saranno riservate a chi ha effettuato l'estrazione ed esegue l'elaborazione. Il file verrà subito trasferito telematicamente sul sistema RedCap di Careggi. L'applicazione è su un server aziendale dell'Azienda Ospedaliera-Universitaria di Careggi ma è accessibile da remoto. Su RedCap non verrà inserito nessun dato direttamente identificativo degli interessati. Una volta trasferito il file sull'applicazione RedCap, esso verrà immediatamente cancellato dal File Server di Villa Serena.

Relativamente alla elaborazione statistica dei dati raccolti, un volta trasferiti su Redcap essi saranno trasformati in variabili qualitative e quantitative per poterle elaborare con dati statistici. In pratica, per quanto riguarda la scelta del metodo di analisi, oltre alla classica statistica descrittiva utilizzata per organizzare e descrivere il campione pervenutoci, sarà eseguita:

- la frequenza e la relativa distribuzione in percentuale di frequenza e/o la categorizzazione in classi
- gli indici di tendenza centrale: soprattutto la media
- le relative misure di variabilità

Questi dati e i calcoli verranno effettuati tutti tramite RedCap con i relativi grafici e le relative tabelle. In seguito, avendo dati qualitativi e dati quantitativi, si valuterà se applicare la statistica del Test del Chi-Quadrato; lo studio si effettuerà raggruppando i dati in categorie (variabili) per scoprire se i dati pervenuteci sono casuali o significativi e supportati a livello statistico. Confronteremo i dati della statistica con i risultati della tavola dei valori critici del Chi-Quadrato considerando il grado di libertà della formula. I valori critici presi in considerazione nello studio saranno 0,05 e 0,01. Sapendo che il metodo del Test del Chi Quadrato può essere applicato a numeri totali maggiori o uguali a 5 e non sapendo fino alla elaborazione dei dati se con le variabili che andremo a studiare totalizzeremo questo numero(in quanto andremo a valutare tutte le scale di valutazione utilizzate (EBS, NPI ecc) che hanno utilizzato a Villa Serena per prendersi cura degli anziani ricoverati, si è ipotizzato di decidere in seguito la scelta del metodo di analisi appropriato in base ai dati. Qualora non si potesse utilizzare il Test del Chi Quadrato si farà ricorso ad altri metodi di statistica inferenziali.

I dati, una volta elaborati ed aggregati, saranno inviati agli altri co-sperimentatori compressi tramite formato RAR con il programma 7ZIP, il quale permette l'accesso alla consultazione solo tramite apposita Password. Il codice di accesso di sicurezza sarà inviato precedentemente tramite PEC con FEQ (firma elettronica qualificata).
La compiuta anonimizzazione dei dati sarà nuovamente verificata nella prospettiva della pubblicazione secondo la tecnica della K anonimizzazione prevedendo un valore K pari a 4.
Nel caso in cui il valore sia inferiore a 4, si procedrà ad aumentare la classe di riferimento.

Indicare dove vengono archiviati i dati[9]

Durante l'elaborazione dei dati, questi saranno custoditi nell'applicazione RedCap. I dati estratti, una volta trasferiti sull'applicazione saranno cancellati definitivamente dalla RSA Villa Serena.

Indicare se i dati sono trasferiti (si/no) ed eventualmente dove: (fuori dall'Azienda, fuori dall'Italia, fuori dall'Unione Europea)[10]

I dati non vengono trasferiti Extra UE

PRINCIPI FONDAMENTALI

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

La base giuridica del trattamento, per gli interessati per i quali sarà possibile ottenere un consenso (dai soggetti di cui all'art. 82 comma 2 del Codice), è rappresentata dal consenso; per gli altri, verosimilmente in numero maggiore, sarà 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 utilizzati[12]

I dati raccolti sono solo quelli indispensabili per procedere alle elaborazioni (test, scale) previste dal protocollo.

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

I dati saranno conservati per 7 anni. Siamo consapevoli 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 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, in particolare per uno studio che mira ad una valutazione di qualità ed efficacia di una metodologia di trattamento che sarà verosimilmente utilizzata per diversi anni.

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]

Il software Cartella Utente Web consente di estrapolare i dati direttamente su un foglio Excel che viene salvato direttamente sul File Server di Villa Serena in una cartella nominativa che necessita, per l'accesso, di credenziali personali; il file Excell sarà trasferito sull'applicazione RedCap. I dati raccolti non sono dunque soggetti a trascrizioni o interpolazioni manuali che potrebbero determinare una loro errata duplicazione.

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 accidentali[15]

Durante l'elaborazione dei dati questi saranno custoditi nell'applicazione web RedCap; precedentemente, come già osservato, vengono estrapolati ed inseriti nel portale della RSA Villa Serena denominato File Server, un server della struttura in cui è possibile effettuare delle archiviazioni centralizzate. Il sistema prevede delle cartelle nominali e solo l'intestatario della cartella può accedervi con un nome utente ed una password personali. L'utente abilitato all'accesso ai dati della ricerca è uno soltanto su ambedue i sistemi.

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

I dati sono pseudonimizzati una volta estratti dalla cartella clinica elettronica di Villa Serena. Ad ogni paziente arruolato sarà assegnato un codice strutturato come segue:

- Mario Rossi nato nel 1939 a.....
- Maria Bianchi nato nel 1940 a...

Il signor Mario Rossi una volta estrapolato dal database verrà convertito in una variabile ipotizziamo X1, la signora Maria Bianchi in una variabile ipotizziamo la X2. Anno 1939 diventerà la nostra variabile Y, anno 1940 diventerà la nostra variabile Y1 e così via. Per cui X1Y ..., X2Y1...
Ai fini dello studio è utile registrare sono l'anno di nascita.

In seguito i dati sono anonimizzati prima della pubblicazione, secondo la tecnica della K anonimizzazione prevedendo un valore K pari a 4. Nel caso in cui il valore sia inferiore a 4, si procedrà ad aumentare la classe di riferimento.

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono crittografati, e secondo quali modalità[17]

No

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

I dati sono anonimizzati prima della pubblicazione, secondo la tecnica della K anonimizzazione prevedendo un valore K pari a 4

Indicare se i dati sono soggetti a partizione[19]

No

Indicare con quali misure e cautele viene effettuato il trasferimento dei dati[20]

Vedere sopra

Indicare i criteri di profilazione per l'accesso ai dati[21]

Un unico soggetto verrà profilato per accedere ai sistemi ed effettuare le elaborazioni

Indicare se gli accessi sono tracciati[22]

Gli accessi non sono tracciati tramite il portale File Server, sono tracciati tramite l'applicazione RedCap.

Indicare con quale frequenza viene effettuato il backup dei dati[123]

Su RedCap dati vengono sottoposti a backup giornaliero, con possibilità di rapido *restore* in caso si verifichi una modifica indesiderata

Indicare se il sistema prevede misure contro virus e malware[24]

Sì

Indicare se i dati sono trattati anche su supporti cartacei, e come questi sono gestiti[25]

I dati saranno trattati sono con formati informatizzati e si prevede una gestione di supporti cartacei solo nel caso di pazienti per i quali sia possibile acquisire il consenso dei soggetti di cui all'art. 82 comma 2 del Codice

DIRITTI DEGLI INTERESSATI

Ove applicabile: indicare come sono informati gli interessati al trattamento

Il periodo di retrospezione ritenuto utile per la ricerca è pari a 10 anni.

Il numero dei pazienti che si intende arruolare risulta essere pari a 500.

Relativamente agli sforzi che si intenderebbe svolgere per provare a contattare i pazienti ritenuti persi al *follow up* ovvero come accertarne l'avvenuto decesso, sono state effettuate verifiche presso l'archivio dei deceduti di Villa Serena, dalle quali sono risultati deceduti 350 pazienti; per i restanti 150 dei 500 previsti come arruolabili, è stata verificatol'esistenza dei dati di contatto e per essi si procederà pertanto, laddove effettivamente contattabili, a mettere a disposizionele informazioni ex art. 13 e acquisirne il consenso al trattamento (laddove incapaci, dai soggetti di cui all'art. 82 comma 2 del Codice).

Se dopo 3 tentativi di contatto telefonico il paziente non risponde, verrà considerato non contattabile e quindi arruolato nello studio in base alla procedura di consultazione preventiva in esame.

Per i pazienti contattabili (verosimilmente, i soggetti di cui all'art. 82 comma 2 del Codice), verrà proposta una informativa e richiesto un consenso per il trattamento dei dati.Per gli interessati non contattabili, si prevede di rendere disponibile l'informativa sullo studio recante gli elementi di cui all'art. 13 e 14 del Regolamento UE 2016/679, anche ai sensi dell'art. 9 par. 4 del Regolamento UE 2016/679 e nel rispetto dell'art. 6 comma 3 delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, mediante pubblicazione sul sito istituzionale dei due titolari del trattamento per tutta la durata dello studio stesso.

Ove applicabile: indicare come è acquisito il consenso degli interessati

Per i pazienti contattabili, nei casi in cui l'interessato, per motivi di salute riconducibili alla gravità dello stato clinico in cui versa, non sia in grado di recepire le indicazioni rese nell'informativa e di prestare validamente il consenso, dato atto che le finalità dello studio non possono essere conseguite mediante il trattamento di dati riferiti a persone in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso o con altre metodologie di ricerca, viene acquisito il consenso delle persone indicate nell'art.82, comma 2, lett. a, del Codice (chi esercita legalmente la rappresentanza, prossimo congiunto, familiare, convivente o unito civilmente, fiduciario oppure in loro assenza responsabile della struttura presso cui dimora l'interessato).

Ove applicabile: indicare se gli obblighi del responsabile del trattamento sono chiaramente definiti e formalizzati, e in caso di risposta positiva precisare come[26]

Nessun soggetto è individuato come responsabile del trattamento ai sensi dell'art. 28 par. 3 del regolamento UE 2016/679

Valutare se, in caso di trasferimento dei dati al di fuori della UE, i dati godono di una protezione equivalente[27]

I dati non vengono trasferiti extra UE

GESTIONE DEI RISCHI
ACCESSO ILLEGITTIMO AI DATI
Indicare una stima della probabilità e gravità del rischio (indefinita, trascurabile, limitata, importante, massima), anche alla luce delle misure pianificate, 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 una stima della probabilità e gravità del rischio (indefinita, trascurabile, limitata, importante, massima), anche alla luce delle misure pianificate, 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 una stima della probabilità e gravità del rischio (indefinita, trascurabile, limitata, importante, massima), anche alla luce delle misure pianificate, 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 (principal investigator)

.....Dr.ssa Antonella Notarelli.....
SOD Neurologia 1
Centro Ricerca e Innovazione Demenze
AOU Careggi

1L'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 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). Il Preposto al trattamento, in Azienda, è, per quanto riguarda gli studi, il PI.

2Inserire titolo e codice dello studio.

3Finalità 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.

4In 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 (cioè di una loro stretta funzionalità rispetto allo studio).

5L'interessato è la persona fisica cui si riferiscono i dati personali trattati: in uno studio, sono i pazienti in essi arruolati, descritti attraverso le caratteristiche (es. di patologia, esiti, età) che li rendono in esso eleggibili.

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

Tali soggetti dovrebbero essere stati istruiti sulle corrette modalità di trattamento dei dati, e 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), essere raccolte in un atto di nomina a firma del P.I. (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).

La persona autorizzata al trattamento è insomma 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.

7Qui si può far riferimento tanto ad altri Centri di sperimentazione, che partecipano allo studio quali titolari autonomi o contitolari del trattamento, che 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 elaborazione e condivisione del protocollo di ricerca, e che quindi devono formalmente individuarsi – mediante un atto o contratto - come Responsabili del trattamento (è 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).

8Un 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.).

La 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.

9E' necessario individuare dove i dati vengono allocati per la gestione dello studio, specificando anche il sistema o il data base utilizzato. Se per la loro successiva conservazione si utilizza una banca dati diversa, occorrerà indicarla. In ordine ai profili di sicurezza, anche in relazione alla integrità dei dati, è inutile precisare che un foglio excel su un pc in locale non soddisfa i requisiti minimi.

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, allegandolo o meno, nel presente documento).

10Si precisa nuovamente che il trasferimento del dato coincide con il suo mero spostamento anche all'interno di un singolo ambito di titolarità (cioè ad es. da un server all'altro dell'Azienda).

11Nel 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.

12La 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.

13Il termine previsto è ordinariamente di sette anni, un termine maggiore (ad es. assolutamente necessario per un registro di patologia) deve essere motivato..

14In questo caso l'esattezza del dato non si intende riferita al suo aggiornamento, ma alle modalità con le quali i dati sono raccolti e dunque duplicati, garantendone appunto l'esattezza rispetto ai dati originali, 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.

15Ai 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.

16 La pseudonimizzazione 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 strutturato e gestito il processo di pseudonimizzazione dei dati.

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

18L'informazione non è relativa alla ovvia anonimizzazione dei dati che si effettua in vista della pubblicazione dei dati di studio, operazione successiva alla chiusura dello studio (o comunque di una sua fase). 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, ricollegato all'interessato. Come tale, il dato anonimo/anonimizzato ben raramente può essere presente in uno studio. 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, normalmente, 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).

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

20Il 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.

421La 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; 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 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, se sono tracciati anche gli accessi in consultazione, per quanto tempo gli eventuali file di log sono conservati.

23Tra 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.

24Il 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.

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

26Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Più in concreto: il responsabile è il soggetto al quale il titolare esternalizza una attività o un servizio, che comporta un trattamento di dati personali che sono nella Titolarità di quest'ultimo. 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.

27Si pone qui la questione del trasferimento dei dati extra UE, 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.