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]

Nome studio:

Validation of Pixyl lesion segmentation method, an Automated Statistical Technique for Counting Distinct Multiple Sclerosis Lesions

Indicare la finalità del trattamento[3]

Validazione di un metodo di segmentazione automatica di lesioni confluenti evidenziate dalla Risonanza Magnetica, in pazienti affetti da Sclerosi Multipla, nell'analisi longitudinale Pixyl.neuro.

Per ogni paziente saranno analizzate le Risonanze Magnetiche eseguite per controllo come da pratica clinica, saranno identificate le aree di iperintensità nelle sequenze T2 pesate indicative di danno da Sclerosi Multipla, e per ogni area di iperintensità nelle sequenze T2 pesate saranno calcolati il numero di singole lesioni da Sclerosi Multipla che confluiscono in quelle aree. Tali lesioni saranno calcolate da due operatori umani esperti nell'analisi di RM, e da due software automatici: il software sviluppato da Pixyl.neuro e quello sviluppato da Dworkin e collaboratori.
Lo studio prevede la valutazione:

- dell'inter-rater variability tra due operatori
- dell'agreement tra gli operatorie l'algoritmo di segmentazione automatica delle lesioni (Pixyl.neuro)
- dell'agreement tra gli operatori e l'algoritmo di segmentazione ideato e validato da Dworkin e collaboratori.

Indicare le tipologie di dati oggetto del trattamento, specificando ogni tipologia di dato[4]

Per ogni paziente saranno valutati soltanto due tipologie di dati radiologici:

- nome dell'area iperintensa nelle sequenze T2 pesate (variabile nominale)
- numero di lesioni calcolate per ogni area di iperintensità calcolate da operatore 1
- numero di lesioni calcolate per ogni area di iperintensità calcolate da operatore 2
- numero di lesioni calcolate per ogni area di iperintensità calcolate da sistema di analisi automatico ideato da Dworkin e collaboratori
- numero di lesioni calcolate per ogni area di iperintensità calcolate da sistema di analisi automatico ideato da Pixyl.

I dati trattati sono qualificabili come dati relativi alla salute

Indicare le tipologie di interessati al trattamento[5]

Pazienti affetti da Sclerosi Multipla recidivante o progressiva diagnosticati secondo i criteri di Poser e McDonald.

Indicare i soggetti interni che partecipano al trattamento quali persone espressamente designate o autorizzate e se queste siano state adeguatamente istruite sul trattamento[6]

Oltre al P.I., medici in formazione specialistica e dottorandi, appartenenti al gruppo di ricerca, adeguatamente istruiti sulle corrette modalitàdi trattamento dei dati.

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]

Istituto Pixyl Medical, La Tronche, France, quale autonomo titolare 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]

Per ogni paziente vengono selezionate le Risonanze Magnetiche analizzabili ed includibili nello studio; i relativi files digitali (acquisiti nel formato DICOM) sono stati archiviati su un server aziendale come da normale pratica clinica.
I files DICOM vengono estratti dal server aziendale e successivamente convertiti in formato .NIFTI mediante l'utilizzo del programma MRI convert; in questa fase i dati saranno pseudonimizzati, assegnando ad ogni RM un codice alfanumerico.
I files .NIFTI pseudonimizzati saranno poi inviati all'Istituto Pixyl Medical tramite l'utilizzo dell'FTP server FileZilla. A questo punto sia il gruppo di ricerca dell'AOU Careggi , sia dell'Istituto Pixyl Medical eseguiranno in cieco la conta manuale delle singole lesioni da Sclerosi Multipla, le quali formano aree iperintense nelle sequenze T2 pesate.
La conta delle singole lesioni da Sclerosi Multipla sarà effettuata da due operatori del gruppo di ricerca dell'AOU Careggi manualmente. I due operatori eseguiranno l'analisi in cieco.
La conta delle singole lesioni da Sclerosi Multipla sarà effettuata dall'Istituto Pixyl Medical mediante l'utilizzo di un software, ideato per questa analisi, e oggetto di validazione nel presente studio.
Gli operatori riporteranno in CRF il numero di singole lesioni, contenute in ogni singola area iperintensa nelle sequenze T2.

Indicare dove vengono archiviati i dati[9]

I dati saranno archiviati sulla piattaforma RedCap.

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

I dati saranno trasferiti l'Istituto Pixyl Medical, La Tronche, France, per l'esecuzione dell'analisi.

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 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. Per i pazienti contattabili, la base giuridica del trattamento è rappresentata dal consenso ex art. 9 par. 2 lettera a) del Regolamento 2016/679.
Minimizzazione dei dati: indicare i criteri utilizzati per garantire l'adeguatezza, la pertinenza e la non eccedenza dei dati utilizzati[12] Lo scopo dello studio in oggetto è la validazione di un metodo di segmentazione automatica per la conta delle singole lesioni di Sclerosi Multipla nelle aree iperintense nelle sequenze T2 pesate di Risonanza Magnetica: conseguentemente, i dati raccolti ed analizzati dagli sperimentatori sono, appunto, le lesioni di Sclerosi Multipla nelle aree iperintense nelle sequenzeT2 pesate di Risonanza Magnetica. Nessun altro dato, oltre a questi, indispensabili, sarà raccolto.
Limitazione della conservazione: indicare per quanto tempo sono conservati i dati e i criteri per la conservazione dei dati[13] Circa il termine di conservazione dei dati fissato a 7 anni, si ribadisce 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 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 per successive verifiche o richieste di precisazioni circa i risultati pubblicati.
Esattezza dei dati: indicare le misure individuate per aggiornare, correggere o cancellare i dati che risultano non esatti in riferimento alla finalità per la quale sono trattati[14] Il dato numero di lesioni nelle aree iperintense nelle sequenze T2 pesate di Risonanza magnetica viene riportato manualmente in CRF dallo sperimentatore che esegue l'analisi, sia essa manuale o automatica. Lo stesso sperimentatore verificherà che il dato sia stato inserito in CRF in modo corretto.
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] Le misure sono rappresentato sostanzialmente da una stretta profilazione degli accessi e dalla pseudonimizzazione dei dati.

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

I file DICOM vengono estratti dal server aziendale, saranno convertiti in formato .NIFTI mediante l'utilizzo del programma MRI convert, in questa fase i dati saranno pseudonimizzati, e ad ogni RM sarà assegnato un codice alfanumerico.

La pseudonimizzazione dei dati avverà attraverso l'assegnazione di un codice alfanumerico (es. Patient_1, Patient_2, ecc.).. I dati personali sono trattati in associazione con questa informazione non direttamente identificativa, e la correlazione tra questa e i dati identificativi dell'interessato è conservata separatamente, accessibile al solo personale coinvolto nello studio, assicurandone, con idonee misure di sicurezza tecniche ed organizzative, la riservatezza.

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

I dati non saranno cifrati

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]

I dati di Risonanza Magnetica pseudonimizzati saranno trasferiti presso l'Istituto Pixyl Medical mediante FTP server con l'utilizzo del software FileZilla.

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

Ogni sperimentatore avrà le stesse prerogative d'accesso ai dati (lettura/scrittura)

Indicare se gli accessi sono tracciati[22]

Si

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

6 mesi

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

Tutti i computer sono aggiornati all'ultima versione del sistema operativo e sono dotati di efficaci software antivirus aggiornati volti a contrastare eventuali attacchi da parte di virus e malware

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

Saranno su supporto cartaceo gli atti di informativa/consenso per i pazienti che sono contattabili

DIRITTI DEGLI INTERESSATI

Ove applicabile: indicare come sono informati gli interessati al trattamento

Una informativa scritta redatta ai sensi dell'art. 13 del Regolamento verrà sottoposta agli interessati al momento della proposta di arruolamento nello studio clinico; per quanto riguarda gli interessati che non è possibile informare, una informativa redatta ai sensi dell'art. 14 del Regolamento sarà pubblicata sul sito istituzionale dell'Azienda.

Ove applicabile: indicare come è acquisito il consenso degli interessati

Ove applicabile il consenso informato verrà acquisito mediante firma cartacea

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

Non sono previsti Responsabili del trattamento

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

Non verranno trattati al di fuori dell'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.

21/12/2023

VALUTAZIONE DEL PREPOSTO AL TRATTAMENTO
Professor Luca Massacesi

……

FIRMA 	

[1] 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 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.

[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.

[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 (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 i pazienti in essi 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.
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.

[7] Qui 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 estern o 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).

[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.).
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.

[9] E' 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).

[10] Si 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).

[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.

[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.

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

[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 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.

[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.

[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.

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

[18] L'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).

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

[20] 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.

[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; 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.

[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 troian , 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] Il 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.

[27] Si 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.