La DPIA (Data Protection Impact Assessment) – o anche VIP (Valutazione d'Impatto Privacy) - è un processo (che esita in un documento) inteso a descrivere il trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento, valutando detti rischi e determinando le misure per affrontarli. E' strumento e conseguenza della responsabilizzazionedeltitolare,esiriferisceauntrattamentoconosciutoanaliticamenteedescrittoinognisuo aspetto; essa, perciò, assume anche una valenza organizzativa, con positiva ricaduta sul piano operativo e logistico dello studio, in particolare se osservazionale (uno studio, cioè, che si risolve esclusivamente nella raccolta ed elaborazione di dati per lo più personali. La DPIA mette dunque a disposizione, in generale:

- unadescrizionesistematicadeltrattamento;
- laesplicitazionedellefinalitàdeltrattamento;
- unavalutazionedellanecessitàeproporzionalitàdeltrattamento;
- unavalutazionedeirischiperidirittielelibertàdegliinteressati;
- lemisuretecnicheeorganizzativecheiltitolareritienedidoveradottarealloscopodimitigaretalirischi.

La DPIA è redatta dal preposto al trattamento[1] e oggetto di parere da parte del Responsabile della protezione dei dati.

DESCRIZIONEDELTRATTAMENTODEIDATI
Indicareladenominazionedeltrattamento[2] "Sicurezza ed efficacia di Ziconotide per via intratecalenella gestione del dolore: uno studio multicentricoretrospettivo" - Codice Protocollo: L2-336.
Indicarelafinalitàdeltrattamento[3] Lo scopo principale dello studio è quello di valutare la sicurezza dello ziconotide, mentre l'obiettivo secondario è analizzarne l'efficacia nella gestione del dolore cronico
Indicareletipologiedidatioggettodeltrattamento,specificandoognitipologiadidato[4] Età; Sesso; Regione di residenza; Centro di impianto; Diagnosi del dolore; Durata del dolore; Mese/anno dell'impianto Z-ITA; Sospensione del trattamento (sì/no, quando, motivi, durata); Intensità del dolore (valori basali, valori dopo il trattamento); Comorbidità (tipologia, numeri); Effetto avverso (tipo, numeri, gravità, frequenza);CPKnelsangue(valoribasali,valoridopoiltrattamento);Usodioppioidi(dosaggibasali,dosaggi dopoiltrattamento);Velocitàdititolazione;Qualitàdellavita(valoribasali,valoridopoiltrattamento).
IltrattamentoricomprendeI'utilizzodistrumentidiIntelligenzaArtificiale?SeSIqualèlalogica di funzionamento? Si, verrannoutilizzati strumentidiIntelligenzaArtificiale per garantirela protezione deidatiintempo reale da minacceinformatiche(es. virus, malware):ifilecontenentidatisonomonitoratitramitesistemidirilevamento proattivodelleminacce basatisuintelligenzaartificiale,cheidentificano comportamentisospetti eattivano automaticamentemisuredicontenimento.
Indicareletipologiediinteressatialtrattamento[5] Pazientiadulti(≥18anni)condiagnosididolorecronico,indipendentementedall'eziologia,sottopostia trattamentoconziconotidemedianteimpiantodaalmenounmese.
Indicareisoggettiinternichepartecipanoaltrattamentoqualipersoneespressamentedesignateo autorizzate[6]

Losperimentatoreprincipaleedisuoicollaboratori.Tuttoilpersonalecoinvoltonellostudiosarà adeguatamente istruito, a cura dello Sperimentatore principale, sul trattamento dei dati.
Indicareeventualisoggettiesternichepartecipanoaltrattamentoqualititolari,responsabiliopersone designate/autorizzate al trattamento[7] IstitutoEuropeoOncologico,IEO(centrocoordinatore);FondazioneISAL(promotore)
Descrivereilflussodati(cioècomeidatisonospostatioelaborati).Occorredescrivereilflusso analiticamente nei suoi vari passaggi, operazioni, attori[8] Ilflussodeidatiprevistoperlostudiomulticentricoretrospettivosiarticolanelleseguentifasi,conindicazione delle operazioni svolte e dei soggetti coinvolti: 1. Identificazione dei soggetti eleggibili – Presso ciascun centro partecipante, una persona appositamente incaricata(diseguito"IncaricatodelCentro")accede alle cartelle cliniche dei pazienti sottoposti a impianto di ziconotide per individuare i soggetti che soddisfano i criteri di inclusione definitinelprotocollodistudio.L'accessoaidaticlinici:avvienetramiteisistemiinformaticiinternidel centro, nel rispetto delle policy di sicurezza e riservatezza interne al centro stesso. 2. Estrazionedeidatirilevanti –L'IncaricatodelCentroestrapoladallacartellaclinicaesclusivamentei dati pertinenti e necessari ai fini dello studio, come specificato nel protocollo. Durante questa fase i dati sono ancora in forma identificativa e non vengono trasferiti all'esterno. 3. Pseudonimizzazione dei dati – Prima dell'inserimento nella piattaforma di raccolta dati, l'Incaricato del Centro provvede a pseudonimizzare i dati, sostituendo ogni informazione identificativa diretta (es.nome,cognome,codicefiscale,numerodicartella clinica)conuncodiceunivocoassegnatoal paziente. L'elenco di corrispondenza tra il codice e i dati identificativi resta conservato esclusivamente all'interno del centro, protetto secondo le misure di sicurezza interne, e non viene mai condiviso con Fondazione ISAL o altri attori esterni. 4. InserimentodeidatinellaeCRF–Idatipseudonimizzativengonoinseritidall'IncaricatodelCentroin una case report form elettronica (eCRF) realizzata in formato Excel, collocata su un ambiente protetto OneDrive di Fondazione ISAL. L'accesso alla eCRF è protetto da password, che viene comunicata separatamente e in modo sicuro all'Incaricato del Centro. L'accesso al file è limitato esclusivamente ai soggetti autorizzati, individuati come parte del team di ricerca. 5. Verifica della qualità dei dati – Fondazione ISAL, in qualità di promotore dello studio, accede alla eCRF per verificare la completezza e la qualità dei dati caricati. In questa fase non viene trattata alcunainformazioneidentificativa,essendopresentinellaeCRFsolodatipseudonimizzati.Eventuali chiarimenti o richieste di integrazione vengono gestiti tramite comunicazioni dirette tra Fondazione ISAL e l'Incaricato del Centro. 6. Analisistatistica–Unavoltacompletatalafasediraccoltaevalidazione,FondazioneISALprocede ad elaborare i dati in forma aggregata, secondo quanto previsto dal piano statistico definito nel protocollo di studio. I dati analizzati non consentono l'identificazione diretta o indiretta dei singoli partecipanti.
Indicaredovevengonoarchiviatieconservatiidati[9] I dati pseudonimizzati contenuti nella eCRF vengono conservati su OneDrive di Fondazione ISAL, con accessocontrollatoetracciato.Laduratadellaconservazioneseguequantostabilitonelprotocolloenella normativa vigente, dopo di che i dati verranno eliminati o anonimizzati in maniera irreversibile. Riguardo alla localizzazione dei dati, oneDrive è un repository cloud incluso nella suite Microsoft 365. Fondazione ISAL utilizza un tenant Microsoft 365 configurato per l'Unione Europea. In base alla documentazioneMicrosoft,idatiarchiviatisuOneDrive/SharePointpertenantUEsonoospitatiindata centersituatiall'internodell'UnioneEuropea,prevalentementeinIrlandaePaesiBassi,nelrispettodel GDPR.
PRINCIPIFONDAMENTALI[10]

Limitazionedellefinalità:indicarelabasegiuridicadeltrattamento,cioèlasuafinalitàlecita,qualeprevista exartt.6e9delRegolamentoUE2016/679(d'orainpoiRegolamento)[11]

Labasegiuridicadeltrattamentoèrappresentatadalconsensoinformatodell'interessato,acquisitosecondo le procedure dei singoli centri partecipanti. Nel caso di una parte dei centri coinvolti, in particolare IRCCS, i pazienti, almomentodell'ingresso,forniscono unconsenso generale all'utilizzo deipropridatiperfuturistudi diricerca clinica, inclusoil presente studio retrospettivo.Intutti gli altri casi, saràrichiestospecificamente un consensoinformatoperlapartecipazioneallostudio.Nonsonoprevistederoghe:idatidipazientidecedutio irreperibili non saranno raccolti né trattati in alcun modo.
Iltrattamentodeidatièquindilecitosolosullabasedelconsensoespressodall'interessato,inconformità allanormativavigentesullaprotezionedeidatipersonali.

Minimizzazionedeidati:indicareicriteriutilizzatipergarantirel'adeguatezza,lapertinenzaelanon eccedenzadeidatiutilizzati[12]

Ai sensi dell'art. 5, paragrafo 1, lett. c) del Regolamento (UE) 2016/679, i dati raccolti e trattati nello studio sono adeguati, pertinenti e limitati a quanto strettamente necessario per il raggiungimento delle finalità di ricerca.
Inparticolare,leinformazioniraccolte(esplicitatealsecondopuntodellasezione"DESCRIZIONEDEL TRATTAMENTO DEI DATI") sono espressamente previste dal protocollo dello studio e ritenute indispensabili per valutare in modo completo la sicurezza e l'efficacia del trattamento.

Limitazionedellaconservazione: indicareperquantotemposonoconservatiidatieicriteriperla conservazione dei dati[13]

Ilterminediconservazionedeidatièfissatoa15anni(25anniperlosponsor);sievidenzialaconsapevolezza che, per gli studi osservazionali, la valenza normativa deitermini di conservazione previsti dalle disposizioni vigenti,sempreorientatearegolareglistudiinterventistici,è,senonassente,comunquenondirettamenteed immediatamente prescrittiva, così che viene comunque chiamata in causa la responsabilizzazione del Titolare.
Èstatoquindiritenutoopportunodifferenziareitempidiconservazionecomesegue:

- 15 anni per i centri clinici, quale periodo adeguato per garantire la tracciabilità dei dati necessari a eventuali verifiche interne, audit o controlli da parte delle autorità competenti, assicurando nel contempo la limitazione della conservazione in relazione alle finalità proprie dei centri;
- 25anniperilpromotore(FondazioneISAL)alfinediassicurarelaricostruzionestoricadellostudio,a tutela della trasparenza scientifica e della solidità dei risultati pubblicati.

Al termine dei periodi indicati, i dati saranno cancellati o resi anonimi in maniera irreversibile, impedendo qualsiasi identificazione, diretta o indiretta, dei soggetti coinvolti.

Esattezzadeidati:indicarelemisureindividuateperaggiornare,correggereocancellareidaticherisultano non esatti in riferimento alla finalità per la quale sono trattati[14]

Pergarantirel'esattezzadeidatiintuttelefasidellostudio,sonostateprevistespecificheprocedurefinalizzate a ridurre il rischio di errori derivanti dall'inserimento manuale delle informazioni nella eCRF.
Poiché i dati verranno estratti manualmente dalle cartelle cliniche e successivamente trascritti nella eCRF (Excel su OneDrive), le misure adottate comprendono:

- Formazione preventiva degli incaricati dei centri clinici - Gli operatori preposti alla raccolta dei dati riceverannoindicazionioperativechiaretramiteun datacollectionmanual,chespecificheràqualidati estrarre, come pseudonimizzarli e come inserirli nella eCRF, al fine di ridurre ambiguità e variabilità.
- Doppia verifica dei dati inseriti - Ogni centro clinico effettuerà una revisione interna dei dati inseriti nella eCRF, confrontandoli con ladocumentazione clinica originale per garantirelacorrispondenzae correggere eventuali errori di trascrizione prima della validazione finale.
- Controllo centralizzato da parte del promotore - Fondazione ISAL, in qualità di promotore, eseguirà unaverificadellacoerenzaecompletezzadeidaticaricatinellaeCRF,individuandoeventuali

incongruenze,valorimancantiodatisospetti.Incasodirilevazionedianomalie,losponsorrichiederà chiarimenti e rettifiche al centro di riferimento tramite comunicazioni sicure e tracciabili.

- Tracciabilitàdellemodifiche-Ognimodificaeffettuataaidatinellae CRFsaràdocumentataetracciata, consentendo di ricostruire in qualsiasi momento le correzioni effettuate e le motivazioni sottostanti.
- Criteriodiesclusionedatierrati-Qualoranonsiapossibileverificarelacorrettezzadiundato,questo nonverràinclusonelleanalisistatistiche,alfinedigarantirel'integritàscientificadellostudio.

Questemisureassicuranocheidatiinseritinellae CRFsianofedelialladocumentazioneclinicaoriginale, riducendo al minimo il rischio di errori che potrebbero compromettere la validità dei risultati.

Integritàeriservatezzadeidati[15]: indicare lemisuretecnicheedorganizzativeadottateper garantirela sicurezzadeidatirispettoatrattamentinonautorizzatioilleciti,perdita,distruzioneodanniaccidentali, precisando quanto segue:

Al fine di garantire la sicurezza dei dati personali, prevenendo trattamenti non autorizzati o illeciti, nonché la perdita, la distruzione o il danneggiamento accidentale, sono state adottate misure tecniche e organizzative adeguate, in conformità a quanto previsto dall'art. 32 del Regolamento (UE) 2016/679 (GDPR).

1. Misureorganizzative
   - Accessocontrollatoaidati:l'accessoaidatièconsentitoesclusivamenteapersonaleautorizzato, identificatoeadeguatamenteformato,inbasealprincipiodinecessitàeminimoprivilegio.
   - Formazionedelpersonale:tuttiisoggetticoinvoltinellagestionedeidatiricevonoformazionespecifica in materia di protezione dei dati personali e sicurezza informatica.
   - Gestione dei trasferimenti: i dati sono trasferiti tramite canali sicuri, utilizzando protocolli cifrati e password inviate attraverso canali separati.
2. Misuretecniche
   - eCRFprotetta:l'inserimentodeidatiavvienetramiteunapiattaformaelettronica(eCRF)conaccesso protettodacredenzialiunivocheemeccanismidiautenticazionesicuri.
   - Crittografiadei dati:idatipersonalisono cifratisiainfase ditrasferimento che,ovepossibile,in fase diconservazione,perimpedirnel'accessodapartedisoggettinonautorizzati.
   - Backup periodici: vengono effettuati backup regolari su sistemi protetti per prevenire la perdita accidentale dei dati e consentire il ripristino in caso di incidenti.

Pergarantirel'integritàel'affidabilitàscientificadelleinformazioniraccoltesonopreviste:

- procedurediverificaincrociatatraidatiriportatinelladocumentazioneclinicaoriginaleequelliinseriti nella eCRF;
- controllidiqualitàperiodicicondottidalpromotore;

sistemidivalidazioneautomaticadeidatiperridurreerroridiinserimentomanuale.

Indicareseneltrattamentooinqualchesuafase(specificare)idatisonopseudonimizzati,esecondoquali modalità[16]

La pseudonimizzazione dei dati sarà adottata come misura di sicurezza e minimizzazione deidatipersonali. Fase di pseudonimizzazione: l'operazione viene effettuata al momento dell'estrazione dei dati dalle cartelle cliniche del paziente da parte dell'incaricato del centro clinico, prima dell'inserimento nella eCRF.
Modalità di costruzione del codice: Ad ogni paziente viene assegnato un codice alfanumerico univoco, generatoinmododanoncontenereinformazioniidentificativedirette(nome,cognome,codicefiscale,numero di cartella clinica). Il codice permette di collegare i dati clinici alla persona solo all'interno del centro clinico, che custodisce separatamente la chiave di corrispondenza tra il codice e i dati identificativi.
Gestione del processo: La correlazione tra codice e dati identificativi è accessibile unicamente al personale autorizzato presso il centro clinico. I dati caricati nella eCRF del promotore (Fondazione ISAL) saranno pseudonimizzati, senza alcuna informazione direttamente identificativa, garantendo che il promotore non possa risalire all'identità del paziente.
Misuredisicurezzatecnicheeorganizzative:Conservazioneseparataeprotettadellachiavedidecodifica;

Accesso ai dati e ai codici regolamentato da credenziali univoche e autenticazione a due fattori; Trasferimentodeidatipseudonimizzatitramitecanalicifratiesicuri;Tracciabilitàdiogniaccessoomodifica ai dati pseudonimizzati nella eCRF.

Indicareseneltrattamentooinqualchesuafase(specificare)idatisonocrittografati, esecondoquali modalità (ovvero quale sistema di crittografia è utilizzato)[17]

Nel corso dello studio, i dati non vengono crittografati nella fase di raccolta e gestione locale presso i singoli centri,inquantorimangonoall'internodelperimetrodititolaritàdelcentroesonoprotettidamisuredisicurezza fisiche e logiche. I dati vengono invece pseudonimizzati e, al momento del trasferimento al promotore (Fondazione ISAL), sono trasmessi attraverso la piattaforma OneDrive for Business (Microsoft 365), che utilizza crittografia AES a 256 bit per i dati a riposo e protocollo TLS/SSL per i dati in transito, garantendo la protezione contro accessi non autorizzati durante comunicazioni e archiviazione sul cloud.
Insintesi,lacrittografiaèquindiapplicata:

- Intransito:tramiteprotocolloTLS/SSL(TransportLayerSecurity).
- Ariposo(sulcloud):tramitecrittografiaAES-256,comeprevistodall'infrastrutturaMicrosoft 365.

Indicareseneltrattamentooinqualchesuafase(specificare)idatisonoanonimizzati,esecondoquali modalità[18]

Nel presente studio, i dati personali non saranno anonimizzati durante le fasi di raccolta, gestione e analisi iniziale, in quanto è necessario mantenere l'associazione con i codici pseudonimizzati per garantire la tracciabilità, la verifica della qualità e la completezza dei dati.
Tuttavia, in vista della pubblicazione dei risultati aggregati, i dati saranno trattati con tecniche di anonimizzazione statistica, finalizzate a impedire qualsiasi possibilità di reidentificazione dei singolipazienti.
Fasedianonimizzazione:avverrànellafasefinaledellostudio,primadellaproduzionedidatasetdestinatialla pubblicazione o a condivisione esterna dei risultati.
Tecnicheutilizzate:

- Generalizzazione degliattributi:idatiindividualisarannoaggregatiosintetizzati riducendoildettaglio specifico (ad esempio, intervalli di età, categorie generali per comorbidità o dosaggi).
- K-anonimato: ogni record individuale sarà raggruppato con almeno K = 4 altri soggetti con caratteristiche simili, in modo da garantire che nessun dato possa essere ricondotto a un singolo individuo.
- Soglia minima di sicurezza: tutti i valori presentati nei dataset pubblici rispetteranno la regola della soglia, assicurando che le informazioni siano riferibili a gruppi di almeno quattro partecipanti, eliminando la possibilità di identificazione diretta o indiretta.

Questaproceduragarantisceche,almomentodelladiffusionedeidati,essisianoirreversibilmentede-identificati, senza possibilità di correlazione con le informazioni identificative originali, pur preservando l'utilitàstatisticadeirisultatiperlaricercascientifica.

Indicareicriteridiprofilazioneperl'accessoaidati[19]

L'accessoaidativieneregolatoattraversounsistemadiprofilidiautorizzazionechedefiniscelaprofonditàe l'estensione delle operazioni consentite a ciascun utente, in conformità ai principi di minimizzazione e necessità previsti dal GDPR.
Icriteriadottatiprevedono:

- Accessolimitatoedifferenziatoperruolo,inbaseallespecificheresponsabilitàoperative:
  - Responsabiledellostudio:accessocompletoaidati,conpossibilitàdiconsultazione,modifica, caricamento e gestione dei permessi di altri utenti.
  - Collaboratoriautorizzati:accessosoloinletturaecaricamento,senzapossibilitàdimodificare oeliminareidatiesistenti.
  - Amministratore IT: accesso tecnico alla piattaforma per finalità di manutenzione e sicurezza, senza possibilità di visualizzare il contenuto dei dati.
- Principio del privilegio minimo (least privilege): ogni utente dispone solo delle autorizzazioni strettamente necessarie allo svolgimento delle proprie mansioni.

- ControllocentralizzatodeipermessitramitelapiattaformamicrosoftoneDrive,checonsentedi:
  - assegnareerevocareiprofilidiaccessoinmodopuntuale,
  - tracciarelemodificheaipermessi,
  - monitorareeventualianomaliediaccesso.
- Revisioneperiodicadeiprofilidiaccessopergarantirecheleautorizzazionirimanganosempre coerenti con le funzioni svolte.

Inquestomodo, lagestionedeidatiavvieneinuncontestosicuroecontrollato, riducendoilrischiodi accessi non autorizzati o di trattamenti non conformi.

Indicaresegliaccessisonotracciati[20]

Pergarantirelasicurezza,lariservatezzael'integritàdeidati,vengonoimplementateleseguentimisuredi gestioneecontrollodegliaccessi:

- Autenticazioneaduefattori(MFA)perunlivellodiprotezioneaggiuntivodurantel'accessoalla piattaforma.
- Tracciamentodegliaccessi(auditlog)attivosuOneDrive,cheregistra:
  - identificativodell'utente,
  - dataeoradi accesso,
  - tipologiadioperazionesvolta(consultazione,modifica,download,eliminazione).

I logvengonoconservatiperunperiododi180giorni, inconformitàalleimpostazionidiMicrosoftOneDrivee alle policy interne di sicurezza.
Tracciamento anchedelle sole consultazioni, oltre chedellemodificheaidati, alfinedigarantire la completa rintracciabilità di ogni operazione.
Monitoraggio periodico dei log da parte del responsabile della sicurezza informatica per rilevare eventualianomalie o accessi non autorizzati.
Inquestomodo,vienegarantitalarintracciabilitàelaresponsabilizzazionediogniattivitàsvoltasulla piattaforma,atuteladell'esattezzaedell'integritàdeidatidellostudio.

Riguardo alla tracciabilità delle modifiche ai dati, essa non è garantita dal file Excel in quanto tale, bensì dalla piattaforma Microsoft OneDrive/SharePoint su cui la eCRF è ospitata. In particolare, il sistema registra automaticamente gli accessi al file, le modifiche apportate, l'identità dell'utente che ha effettuato l'operazione,ladatael'oradellamodificaelacronologiadelleversionidelfile(versionhistory). Attraversola funzionalitàdicronologiaversioni,èsemprepossibilevisualizzaree,senecessario,ripristinareunaversione precedente del documento, consentendo quindi di risalire a chi e quando ha effettuato una modifica. Si precisa che il sistema conserva la versione precedente del file nel suo complesso; non è previsto un audit trail cella-per-cella.

Logdiaccessoemodifica
I log di accessoemodifica sonoconsultabili tramite la cronologia versionidel singolo file, il pannello Attività deldocumentoe, pergliutentiautorizzati,tramiteilogdiauditdiMicrosoft365,checonsentonoditracciare eventi quali apertura, modifica, download e condivisione dei file.

Indicareconqualefrequenzavieneeffettuatoilbackupdeidati[21]

IlbackupdeidativienegarantitoattraversolefunzionalitàintegratedelservizioMicrosoftOneDrive,utilizzato come piattaforma di archiviazione e gestione della documentazione elettronica dello studio.
In particolare:

- Il sistema effettua backup automatici e continui, assicurando la protezione dei dati in tempo reale grazieallareplicazionesuserverridondantisituatiindatacenterconformiaglistandarddisicurezzae alle normative europee (es. ISO 27001, GDPR).
- È attivata la funzione di versioning, che consente di recuperare versioni precedenti dei file in caso di modifiche accidentali o cancellazioni.

- Idatisonoprotettidacrittografiasiaintransitocheariposo,riducendoilrischiodiaccessinon autorizzati o perdite durante la trasmissione.

Lafrequenzadibackupècostanteeautomatizzata,senzanecessitàdiinterventimanuali,garantendocosì lacontinuitàoperativael'integritàdelleinformazioni.

Indicareseilsistemaprevedemisurecontrovirusemalware[22]

Il sistema utilizzato per la gestione dei dati, basato su Microsoft OneDrive, prevede misure integrate di protezione contro virus, malware e altre minacce informatiche.
In particolare:

- Protezione integrata di Microsoft 365: OneDrive utilizza sistemi di scansione automatica dei file per rilevare la presenza di virus o malware al momento del caricamento o della sincronizzazione.
- Antivirusefirewallaziendali:idispositiviutilizzatidalpersonaleautorizzatoall'accessoaidatipressoi singolicentriclinicisonodotatidisoftwareantivirusaggiornatiedifirewallattiviperprevenireintrusioni esterne.
- Protezionein temporeale: ifile sonomonitoratitramitesistemidirilevamento proattivodelle minacce basati su intelligenza artificiale, che identificano comportamenti sospetti e attivano automaticamente misure di contenimento.
- Crittografia end-to-end: i dati sono crittografati sia in transito che a riposo, riducendo il rischio di manipolazioni da parte di software malevoli.
- Aggiornamentiautomaticidisicurezza:Microsoftrilasciaaggiornamentiperiodiciepatchdisicurezza che vengono applicati automaticamente, garantendo la protezione costante del sistema.

Indicareseidatisonotrattatianchesusupporticartacei,ecomequestisonogestiti[23]

I dati dello studio sono inizialmente consultati e raccolti dalle cartelle cliniche cartacee custodite presso ciascun centro clinico partecipante.
Lemodalitàdigestionesonoleseguenti:

- Consultazione interna: l'accesso alle cartelle cliniche cartacee è consentito esclusivamente al personale sanitario autorizzato e direttamente coinvolto nello studio, nel rispetto delle procedure interne di ciascun centro.
- TrascrizionemanualenellaeCRF:idatirilevantiaifinidellostudiovengonoriportatimanualmentedal personale autorizzato dall'anagrafica cartacea alla piattaforma elettronica (eCRF), avendo cura di garantire l'esattezza e la completezza delle informazioni trasferite.
- Conservazione protetta: le cartelle cliniche cartacee rimangono archiviate presso i locali di competenza di ciascun centro clinico, in armadi chiusi a chiave o aree accessibili solo al personale autorizzato.
- Assenzadiduplicazioninonnecessarie:nonvengonocreatecopiecartaceeaggiuntivedeidatiestratti, se non quando strettamente indispensabile e comunque nel rispettodelle normesulla protezione dei dati personali.
- Smaltimentosicuro:eventualidocumenticartaceitemporanei(es.appuntidilavoro)vengonodistrutti in modo sicuro, tramite triturazione o altri sistemi idonei, evitando che possano essere recuperati o consultati da soggetti non autorizzati.

DIRITTIDEGLIINTERESSATI

Indicarecomesonoinformatigliinteressatialtrattamento[24]

Perlostudioinoggetto,l'informativaagliinteressatiel'acquisizionedelconsensoavverrannosecondole seguentimodalità:

- Centricheadottanoilconsensopreventivo-Neicentriincuiipazienti,all'ingressoinstruttura,firmano unconsensoinformatogeneraleperl'utilizzodeidatiafinidiricercascientifica,taleconsensocoprirà anchelostudioinquestione.

- Centrichenonadottanoilconsensopreventivo-Pericentrichenondispongonodiquestaprocedura, saràànecessarioinformaredirettamenteipazientieraccoglieréilconsensospecificoallostudioprima di inserire i dati nella eCRF.

Contattiperl'eserciziodeidiritti:Nell'informativasaràindicatocomereferenteilResponsabiledellaProtezione dei Dati (DPO) del centro di sperimentazione, a cui gli interessati potranno rivolgersi per esercitare i propri diritti (accesso, rettifica, cancellazione, limitazione, opposizione).

Questaimpostazioneassicurailrispettodellanormativavigenteegarantiscechevenganotrattatisoloidati per i quali vi sia consenso esplicito e valido, evitando situazioni di impossibilità o sproporzione come previstedall'art.110delD.Lgs.196/2003edalRegolamentoUE2016/679.

Indicareleragionipercuinonèpossibileinformaregliinteressati[25]

Gestione deicasidipazienti deceduti,irreperibili o non contattabili - Non sono previstederoghealconsenso informato.Pertanto,idatidipazientideceduti,irreperibilinoncontattabilinonverrannoacquisitinéutilizzati.

Indicare,perglistudiperiqualièpossibile,comeèacquisitoilconsensodiquotapartedegliinteressati[26]

Ilconsensoèacquisitoinformascritta,sottopostoalpazienteduranteunavisitapressoilcentroe adeguatamente spiegato al paziente stesso.

Indicareseiltrattamentocoinvolgesoggettiqualificaticomeresponsabilideltrattamento[27]

Almomentodell'attivazionedeicentrisatellitipartecipantiallostudiosaràsottoscrittounaccordoprivacyper regolamentare il trasferimento/condivisione dei dati ai sensi del Regolamento EU 679/2016".

GESTIONEDEIRISCHI[28]

ACCESSOILLEGITTIMOAI DATI

Nelcontestodellostudio,leprincipaliminacceindividuateriguardanosialafasediraccoltaeinserimentodati che quelle di archiviazione, trasferimento e consultazione. Le minacce principali sono:

- Erroreumanonellagestionedeidati(es.inserimentomanualeerratootrascrizionescorrettadalle cartelleclinicheall'eCRF).
- Accessononautorizzatodapartedipersonaleinternononinclusonelteamdiricerca.
- Utilizzoimpropriodellecredenziali,comecondivisionedipasswordomancatologout.
- Attacchiinformaticiesterni(es.hacking,phishing,malware,ransomware).
- Intercettazionedeidatiduranteiltrasferimento,incasodiutilizzodicanalidicomunicazionenon protetti.
- Smarrimentoosottrazionedidocumentazionecartaceaodispositivicontenentidati.
- Eventiaccidentalicome incendi,allagamenti,guastihardware chepossanodeterminareperditao compromissione dei dati.

Lefontidirischiochepotrebberofavorirel'accessoillegittimoaidatisonoriconducibiliatreambitiprincipali:

- Fattoriorganizzativi
  - Insufficientedefinizionediruoliresponsabilitàall'internodeicentriclinici.
  - Mancanzadiadeguataformazionedelpersonalesultrattamentodeidatiesullemisuredi sicurezza.
  - Procedureincompleteperlagestionediemergenzeeincidentidisicurezza.
- Fattoritecnologici
  - Vulnerabilitàinformatichedeisistemiutilizzati(es.eCRF,server,dispositivilocali).
  - Mancanzadicifraturaoprotocollisicuriduranteiltrasferimentodeidati.
  - Assenzadisistemiditracciamento(audittrail)permonitorarel'accessoaidati.

- Fattorifisici
  - Accessononcontrollatoallecartelleclinichecartaceecustoditeneicentriclinici.
  - Protezioneinadeguatadilocaliodispositivicontenentidatisensibili.
  - Smarrimentoofurtodidocumentazioneosupportiinformaticiportatili.

Permitigareirischiidentificatisonostateadottatespecifichemisuretecnicheeorganizzative,tracui:

- Controllisugliaccessi
  - Autenticazioneconcredenzialiindividualiedifferenziateperprofilodiautorizzazione.
  - Limitazionedegliaccessifisiciallecartelleclinicheaisolioperatoriautorizzati.
  - Tracciamentodegliaccessilogicitramiteaudittrail,ovetecnicamentedisponibile(es.Microsoft OneDrive).
- Protezionedeidatiduranteiltrasferimento
  - Utilizzodiprotocollisicuri(es.PEC,canalicifrati).
  - Separazionetrainviodeidatiecomunicazionedellechiavidicifratura.
- Misuredisicurezzainformatica
  - Sistemiantiviruseantimalwarecostantementeaggiornati.
  - Backupregolaredeidaticonconservazioneinambientesicuro.
  - Protezionedeidispositiviutilizzatiperiltrattamento(password,bloccoautomatico).
- Misureorganizzative
  - Formazionespecificadelpersonalecoinvoltonellostudio.
  - Procedureinterneperlagestionedicartelleclinichecartaceeperlatrascrizionemanualedei dati.
  - Procedureperlagestionedieventualidatabreach.

Considerandolemisuretecnicheeorganizzativeadottate,la**probabilità**chesiverifichiunaccessoillegittimo ai dati è valutata come **bassa**.

Tuttavia,lafaseditrascrizionemanualeeditrasferimentocostituisceunpuntocriticocherichiedeparticolare attenzione.

Incasodiaccessononautorizzato,leconseguenzesarebberogravi,datalanaturasensibiledeidatisanitari trattati e il potenziale danno agli interessati (violazione della riservatezza e rischio di discriminazione). Tuttavia, tenendo conto delle misure di sicurezza già implementate e di quelle pianificate, il **rischio complessivo è stimato come limitato**, poiché mitigato dall'adozione di processi di pseudonimizzazione e dalla separazione tra dati identificativi e dati sanitari.

Il livello di rischio finale, considerando probabilità e impatto, si colloca in una fascia limitata, ma richiede un monitoraggio continuo, in particolare durante le fasi di inserimento manuale dei dati e di trasferimento verso il promotore, Fondazione ISAL.

MODIFICHEINDESIDERATEDEIDATI

Leminaccechepossonoportareaunamodificanonautorizzataoindesideratadeidatiincludono:

- Erroreumanodurantel'inserimento,modificaocancellazionedeidaticliniciodistudio.
- Malfunzionamentitecnici del sistema informaticoo delle apparecchiature utilizzate per l'elaborazione e l'archiviazione.
- Attacchiinformaticimiratiallacorruzioneoalterazionedeidati,comeransomwareomalware.
- Accessi non autorizzati che permettano la modifica dei dati da parte di soggetti esterni o interni non autorizzati.
- Eventifisiciimprevisti,comeguastihardwareoproblemidirete,chepossonocorrompereifilesalvati.

Lefontiprincipalidirischiosono:

- Operatoriinterni(personaleautorizzato)che,pererroreomancanzadiformazioneadeguata,possano effettuare modifiche non corrette.
- Difettioguastitecnologici,comecrashdeiserver,danneggiamentodidischirigidiointerruzioni improvvise di corrente.
- Softwarenonaggiornatioprividiadeguateprotezioni,chepossonoesseresfruttatidacyberattacchi.
- Mancanzadiprocedurestandardizzateperlagestioneelaverificadellaqualitàdeidatiinseriti.
- Eventistraordinari(es.calamitànaturalioincendi)chepossanocompromettere l'integritàfisicadei serverodeisupporti.

Sonoprevisteleseguentimisurediprevenzioneemitigazione:

- Backupregolareesicurodeidati,converificaperiodicadellapossibilitàdiripristino.
- Sistemaditracciamento(auditlog)cheregistraognimodificaeffettuata,conindicazionedell'utentee dell'orario.
- Controllodegliaccessiinformaticitramitecredenzialiindividualieautenticazioneapiùfattori.
- Aggiornamentoperiodicodelsoftwareeantivirusperridurreilrischiodimalware.
- Procedureoperativestandard(SOP)perl'inserimentoelagestionedeidati.
- Formazione periodica del personale per ridurre gli errori umani e migliorare la consapevolezza sulle buone pratiche di gestione dei dati.
- Verificaperiodicadell'integritàdeidatitramitecontrollidicoerenzaevalidazione.

Grazieallemisureadottate(backup,controllidiaccesso,formazioneemonitoraggio),la **probabilità**cheuna modifica indesiderata avvenga è **limitata**.

Ilrischioresiduoderivaprincipalmentedapotenzialierroriumanioguastitecniciimprovvisi.

L'alterazionedeidaticliniciodistudiopuòcompromettere l'affidabilitàdeirisultati,conconseguenzegravidal punto divista etico,clinico e scientifico. Tuttavia, le misureadottate riduconosignificativamente lapossibilità che un errore o un attacco comporti una perdita di integrità irreversibile. Il mantenimento e il rafforzamento delle misure di sicurezza (backup frequenti, controlli di integrità, audit log) saranno fondamentali per mantenere il rischio limitato e sotto controllo.

PERDITADEIDATI

Leminaccechepossonocausarelaperdita,ilfurtoolacancellazionenonautorizzatadeidatiincludono:

- Attacchiinformaticimirati,comeransomwareohacking,finalizzatialladistruzioneosottrazione dei dati.
- Erroreumano,adesempiocancellazioniinvolontarieoerratagestionedei file.
- Guastihardwareosoftware,comemalfunzionamentidiserver,dischirigidiopiattaformedi archiviazione.
- Eventifisicistraordinari,comeincendi,allagamenti,furtididispositivicontenentidati.
- Smaltimentononcorrettodisupportifisici(es.cartelleclinichecartacee,hard disk).
- Mancanzadibackupaggiornati,chepuòrendereimpossibileilripristinodeidati.

Leprincipalifontidirischioidentificate sono:

- Postazioni di lavoroe dispositivi nonadeguatamente protetti,come computersenzacrittografia o lasciati incustoditi.
- Personaleinternononformatoononpienamenteconsapevoledelleproceduredisicurezza.
- Infrastrutturatecnologicavulnerabile,senon adeguatamenteaggiornataoprivadisistemi di protezione avanzata.
- Trasferimentononsicurodeidati,chepotrebbeesporliaintercettazionidurantelatrasmissione.

- Archivicartaceinonadeguatamenteprotetti,accessibiliapersonenonautorizzate.
- Usoimpropriodidispositivimobili(es.laptop,USB)chepossonoesseresmarritio rubati.

Lemisureadottatepermitigarequestirischiincludono:

- Backupregolariesicurideidati,contestperiodicidiripristinoeconservazioneincloudMicrosoft OneDrive con crittografia.
- Controllodegliaccessilogicitramitecredenzialiindividualieautenticazioneadue fattori.
- Auditlogpertracciaretutteleoperazionidimodificaecancellazione.
- Protezionefisicadegliarchivicartaceiall'internodiciascuncentro,conaccessoconsentitosoloa personale autorizzato.
- Antivirusesistemianti-malwareaggiornatisututtelepostazionidi lavoro.
- Formazionedelpersonaleinmeritoalleproceduredisicurezzaegestionecorrettadeidati.
- Smaltimentosicurodeisupportifisici,tramiteproceduredidistruzionecertificata.
- Utilizzo di connessioni sicure (es. VPN, protocolli crittografati) per il trasferimento dei dati tra centri.

Allalucedellemisuredisicurezzaimplementatela**probabilità**chesiverifichiuneventodiperdita,furto ocancellazionenonautorizzataè**limitata**,grazieallapresenzadibackupregolari,controllidiaccessoe sistemi di sicurezza informatica avanzati.

Le conseguenze di un evento di questo tipo potrebbero essere gravi, poiché la perdita di dati sanitari potrebbe compromettere la continuità dello studio, la sicurezza dei pazienti e la conformità normativa. Tuttavia, la presenza di backup e di procedure di ripristino riduce in maniera significativa la gravità effettiva dell'impatto. Il rischio residuo è quindi limitato, purché vengano mantenuti e monitorati costantemente i sistemi di backup, le procedure di sicurezza e la formazione del personale.

SchematipoaggiornatoaOttobre 2024

ILPREPOSTOALTRATTAMENTO(vedinota1)
(nome/cognome)

Renato Vellucci

FIRMA	RENATOVELLUCCI 20.12.2025 10:28:09 UTC	*Data* *20 dicembre 2025*

[1]IlPrepostoaltrattamento,inAzienda,è,perquantoriguardaglistudi,ilPI.L'art.2-quaterdeciesdelD.Lgs. 30 giugno 2003 n. 196 prevede che, tra le persone autorizzate altrattamento (cfr. nota 6), il titolare possa individuare, per lo svolgimento di specifiche funzioni di coordinamento e orientamento nel trattamento dei dati,personefisiche,cheoperanosottolaloroautorità,aciò"espressamentedesignate".Lapersonafisica "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,utilizzandovarie espressioni (delegato, referenteecc.): in Azienda la si è definita Preposto, con termine derivato dalla normativa in materia di sicurezza del lavoro, e che indica appunto un soggetto che sovraintende ad una data attività (a far intendere che il trattamento dei dati non è mai una attività sganciata da un concreto operare).

[2]Inseriretitoloecodicedellostudio.

[3] Finalità del trattamento vale il suo scopo pratico. Occorre dunque indicare, posto che il trattamento è ovviamentefunzionaleallaesecuzionedellostudio,oltrealloscopodiricercainsensolato(es."Idatisono trattati per scopo diricerca in campo medico …"), quali sono gli scopi che si intendono raggiungere con lo studio medesimo (es. scopo dello studio è verificare …"). Qualora i dati vengano raccolti per una finalità ulteriore(es.dicura,ilchesignificachesarannotrattatiancheconmodalitàidentificativa),occorreintegrare tale specifico elemento nell'informativa sul trattamento dei dati.

[4] Inviageneralesitrattadidatiafferenti allecategorie particolari,es. relativi alla saluteogenetici, edidati comuni (es. dati anagrafici e di contatto). Oltre a questa indicazione più generica, categorica, occorre esplicitare i dati che vengono effettivamenteraccolti; ciò può esserefattocon un gradomaggiore (es. esiti di questo o quell'esame di laboratorio) o minore (es. esiti esami di laboratorio) di analiticità: è comunque preferibile essere più analitici possibile –questi elementi più puntuali sono normalmente già elencati nel protocollo - anche per motivare, se necessario, tali scelte in una prospettiva di minimizzazione (cfr. nota 12), cioè di una loro stretta funzionalità/indispensabilità rispetto allo studio.

[5] L'interessatoè la persona fisica cuisiriferiscono i dati personali trattati:in uno studio,sono adesempio i pazienti in esso arruolati, descritti attraverso le caratteristiche (es. di patologia, esiti, età) che li rendono in essoeleggibili.OccorrequiIndicareancheilrangetemporaleentroilqualesivannoadidentificareipazienti eleggibili allo studio (es. pazienti diabetici trattati dal 1995 al 2020).

[6]E'sufficienteindicareilnumerodeicomponentidelgruppodisperimentazioneelerelativeprofessionalità, senzaindicazioninominative.Perlapersonaespressamentedesignata,cfr.nota1.Lapersonaautorizzata al trattamento è la persona fisica – dipendente o collaboratore - sottoposta, per quanto concerne il trattamentodei dati, alTitolare(cioè l'Azienda), eche tratta dati personali solo nella misurain cuisia stata aciòautorizzataeistruita:leistruzionidelimitanol'ambitoditrattamentoautorizzato,eprecisanolemodalità secondo le quali il trattamento deve essere effettuato. Nessun incaricato può trattare dati senza adeguate istruzioni(chesonounsuodiritto), enessunincaricato,ricevutele,puòeffettuareoperazioniditrattamento ulterioririspettoaquelledaesseconsentite.Taliistruzioni,nell'otticadellaresponsabilizzazionedeltitolare (che consiste nell'applicare i principi previsti all'art. 5 del regolamento UE 2016/679, documentandone le modalitàdiapplicazione),devonoessereraccolteinunattodinominaafirmadelP.I.(attochepotràessere 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]Quisipuòfarriferimento:

- ad altri Centri di sperimentazione, che partecipano allo studio quali titolari autonomi o contitolari del trattamento(ilTitolaredeltrattamentoèilsoggettoche,individuatounafinalità,cioèunoscopopratico, determina le modalità di trattamento dei dati necessarie per raggiungerlo; qualora finalità e modalità sianocondivise,sipuòstabilireunacondizionedicontitolarità,chedeveessereformalizzatamediante un accordo redatto ai sensi dell'art. 26 del Regolamento);
- a soggetti (normalmente enti) che collaborano funzionalmente allo studio (es. un laboratorio esterno che effettui esami previsti dalla ricerca) ma che non assumono il ruolo di titolare del trattamento in quanto non hanno partecipato alla definizione delle finalità e modalità del trattamento – cioè alla elaborazione e condivisione del protocollo di ricerca - e che quindi devono formalmente individuarsi come Responsabili del trattamento (vedi nota 27).

Occorreelencaretalisoggettideve,inriferimentoallostatoattualedellostudio(inalcunistudimulticentrici, ulteriori partecipanti possono aderire al progetto successivamente) con la loro esatta denominazione.

[8]Untrattamentodidatipersonalisitraduceinunflussodiinformazioni,chepuòcoinvolgerevarispazi(es. banchedati), soggettiecc., echepuòsostanziarsiinunaseriedioperazioni(es.laraccoltadeidati, perla quale occorre indicare come essi vengono selezionati e archiviati, ad es. in un foglio di raccolta o in un database; o la loro comunicazione, tra due o più titolari; le modalità di elaborazione ecc.). E' necessario indicareancheseidatisonomeramentetrasferitiall'internodiunostessoambitodititolarità:iltrasferimento deldatoènozionepiùampia,etalvoltadiversa,daquelladellasuacomunicazione,cioèdellatrasmissione del dato ad altro titolare; questa comporta spesso un trasferimento di dati (ma i dati possono essere comunicati anchemettendoli semplicemente a disposizione, senza trasmetterli); si hatrasferimentodi dati siaseidatisonotrasferitialdifuorideisistemiaziendali, siasesonomeramentespostatiancheall'interno del medesimo ambito di titolarità (cioè ad es. da un server all'altro dell'Azienda, o verso un server di un soggetto che agisce per il titolare, quale responsabile del trattamento). Occorre precisare se i dati sono eventualmente trasferiti:

- nell'ambitodell'Azienda
- fuoridall'Azienda
- fuoridall'Italia
- fuoridall'UnioneEuropea

Iltrasferimentodeldato,soprattuttoseeffettuatoaldifuoridelproprioambitodititolarità(chenormalmente corrisponde ad un perimetro presidiato), può rappresentare un momento critico, che necessita l'adozione diidoneemisuredisicurezzatantotecnichecheorganizzative:diquelleappuntospecificamenteriferibilial trasferimentodeldatosirichiedeunabrevedescrizione.Iltrasferimentodeidati(esclusiidatigenetici)deve essere effettato con modalità sicura, anche con strumenti di cooperazione applicativa oppure utilizzando strumentidimessaggisticacheutilizzinocanalidicomunicazioneprotetti(ivicompresalaPEC),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 cooperazioneapplicativaodimessaggisticacheutilizzinocanalidicomunicazioneprotetti(ivicompresala PEC), cifrando i dati e fornendo la chiave di decifrazione attraverso canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati. E' necessario richiamare eventuali agreement redatti per il trasferimento dei dati, e comunque documentare la valutazione della necessità e proporzionalità del trattamento che è stata effettuata.

[9]Sidistinguequitraarchiviazioneeconservazione,indicandoconlaprimavocelatemporaneaallocazione 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 requisitiminimi (laDPIA non otterrà il parere positivo del Responsabile della Protezionedeidatiaziendale,equand'anchevenissetrasmessa,èchenonsaràpossibileottenerela autorizzazione del Garante). Il sistema di archiviazione e conservazione dei dati di studio messo a disposizione dall'Azienda èRedCap;possonoessereutilizzati strumentidiversi,machegarantiscano, allo stesso modo, un tracciamento degli accessi e delle operazioni effettuate e garanzie contro virus, malware ecc..Qualoravengautilizzataunapiattaformaesterna,occorreràprocurarsilerelativeinformazionitecnico 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 vistatecnico, ma deve essere tale da fornire informazioni sufficienti ad effettuare una minima valutazione di adeguatezza, anche con il supporto della componente tecnico-informatica aziendale.

[10] L'art. 5 (Principi applicabili al trattamento di dati personali) par. 1 del Regolamento prescrive analiticamente alcuni principi che assicurano l'adeguatezza del trattamento (cd. principi base del trattamento);laresponsabilizzazionedelTitolareconsisteappuntonelrispettaretaliprincipienell'esserein grado di dimostrare, con idonea documentazione (redatta prima dell'inizio del trattamento, nell'ottica della privacy by design e by defaut) di averli rispettati. Dunque, il titolare del trattamento è responsabile del rispetto dei seguenti principi:

- limitazionedellafinalitàdeltrattamento;
- limitazionedellaconservazionedeidati,
- minimizzazionedeidati;
- esattezzadei dati;
- sicurezzadeidati(integritàeriservatezza).
- trasparenza del trattamento (riguarda anzitutto le informazioni sul trattamento messe a disposizione degli interessati, se ne parla alla sezione successiva relativa ai Diritti degli interessati).

[11]Labasegiuridicaordinariadeltrattamentodeidatiascopodiricercaclinicaèilconsensodegliinteressati, a seguito di idonee informazioni. Il consenso non è necessario se l'interessato non è contattabile, o se si tratta di studio previsto da una norma di legge/da una disposizione regolamentare/ dal diritto UE/dal programma di ricerca sanitaria di cui all'art. 12 bis del D.Lgs. 502/92.

Nelcasochenonsiapossibileinformarel'interessatoedacquisirneilconsenso,esitrattidistudioprevisto daunanormadilegge/daunadisposizioneregolamentare/daldirittoUE/dalprogrammadiricercasanitaria di cui all'art. 12 bis del D.Lgs. 502/92, occorre riportare quanto segue (scegliendo il caso d'interesse):

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

Se il pazientenonècontattabile - perchéidatidicontattosonostati perduti ononsonoaggiornati,oppure il paziente è deceduto, o è preferibile non informarlo per motivi etici (es. il paziente non è informato sulla patologia di cui è affetto) – oppure se i contatti non sono gestibili per oggettiva impossibilità di carattere organizzativo (contattare i pazienti comporterebbe un impegno sproporzionato rispetto alle risorse disponibili), la base giuridica del trattamento, è rappresentata dal parere positivo del comitato etico competente a livello territoriale, nonché dalla applicazione di misure di garanzia sulla sicurezza del trattamento (che qui stiamo appunto specificando).

[12]Laminimizzazionedeidatisitraduceappuntonellagaranziacheidatisiano"adeguati,pertinentielimitati a quanto necessario rispetto alle finalità per le quali sono trattati", art. 5 paragrafo 1 c del Regolamento). Ovvio che tali requisiti non possano essere assolutizzabili, in quanto strettamente funzionali allo scopo di un dato studio: sarà comunque lecito utilizzare, tanto da un punto di vista qualitativo che quantitativo, soltanto le informazioni indispensabili per quel determinato studio. Chi valuta quali dati sono o meno necessari? Ovviamente il Titolare (e per esso, in un progetto di ricerca, il P.I.) che, nell'ottica della responsabilizzazione, dovrà argomentare e sostenere tale valutazione. Nel nostro caso occorre dunque dimostrare che i dati trattati, e già sopra elencati, sono soltanto quelli necessari alla realizzazione dello studio, e non altri.. E' di tale necessità– strettamente correlata alla razionalità dello studio da un punto di vista eminentementescientifico - chedeveessere databrevemente evidenza, anchesoltanto indicando in sintesi che "i dati raccolti sono quelli indispensabili alla esecuzione dello studio". In relazione a certe tipologieparticolaridiinformazioni,ades.quellerelativealleoriginirazzialioallaappartenenzaetnica,può essere opportuno offrire una motivazione più puntuale ed articolata.

[13]Un termine puntuale per la conservazione dei dati utilizzati per gli studi osservazionali non è previsto e dunquequellosceltodeveessereMotivato.Ilterminedeveesserecommisuratoalloscopoprincipaledella conservazione dei dati, che è anzitutto quello di rendere possibili verifiche o controlli della base dati dello studio successivamente alla pubblicazione. Si consiglia di scrivere qualcosa di analogo a quanto segue:

> Il termine di conservazione dei dati è fissato a … (inserire il numero di anni ritenuto necessario)anni;sievidenzialaconsapevolezzachelavalenzanormativadeiterminidi conservazione previsti dalle disposizioni vigenti, sempre orientate a regolare gli studi interventistici, non è direttamente ed immediatamente prescrittiva per gli studi osservazionali,cosìchevienecomunquechiamataincausalaresponsabilizzazionedel Titolare. Sièconsideratoopportunoapplicare aquesto studio osservazionale il termine di … anni in quanto …

Sesiutilizzailterminediprassidi7anni,lamotivazionepuòessereresacomesegue,sostituendol'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 unaprassiconsolidataesoprattuttoritenutosufficienteenoneccedenteinrelazioneallo scopo di consentire eventuali controlli successivi sulla correttezza delle inferenze effettuate nella valutazione dei dati raccolti nel corso della ricerca. Iltermine settennale è commisurato alla opportunità di conservare una base dati statistica per successive verifiche o richieste di precisazioni circa i risultati pubblicati.

Siricordachemediantel'informativaexart.13oexart.14delRegolamentooccorreindicareecomunicare aisoggettiinteressati, che:

- sonoraccoltisoloidatistrettamentenecessariperilperseguimentodellefinalità;
- decorsi i termini di conservazione, i dati personali saranno distrutti, cancellati o resi anonimi (descrivendo i meccanismi per la cancellazione o anonimizzazione dei dati).

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

[14]In questo caso l'esattezza del dato non si intende riferita al suo aggiornamento, ma alle modalità con le quali i dati sono raccoltidalla documentazione originale e dunque duplicati, garantendone appunto l'esattezzarispettoaquella,perlefinalitàdellostudio.Ovviochemisuredicontrollosonomenonecessarie quandol'estrazionedaundatabaseinformaticoavvienequasiautomaticamenteaseguitodell'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'adeguatasicurezzadeidatipersonali,compresalaprotezione,mediantemisuretecnicheeorganizzative 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:

- ladivulgazionedidatipersonaliol'accessoaglistessinonautorizzatioaccidentali;
- lamodificanonautorizzataoaccidentaledidatipersonali(cosìcheidatisonomodificatioincompleti);
- la perdita della possibilità di accesso o distruzione accidentale o non autorizzata di dati personali.

Occorreindicare,sinteticamente, lemisureadottatedaunpuntodivistaorganizzativo,nonchéquelle informatiche assicurate dal sistema sul quale i dati sono archiviati, anche attraverso il rimando alla relativadocumentazionetecnica.E'ovviochelamodifica,laperditaolanonaccessibilitàaidatisono 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 caratterenonidentificativo(ades.uncodice),sostituendoconessaquelladicaratteredentificativo,ades. ilnome/cognomedell'interessato,emantenendoriservata,conspecifichemisuredisicurezza,lacorrezione tra dato identificativo e dato non identificativo (tra anagrafica e codice). Essa è una operazione di trattamento che si traduce in una misura di sicurezza e di minimizzazione dei dati. Non ogni codificazione può tradursi in una pseudonimizzazione dei dati: non lo è certo l'utilizzo del codice fiscale (ben più identificativo del mero nome giuridico), ma neppure un codice che sia conosciuto al di fuori del gruppo di sperimentazione (es. il numero nosologico o simile, anche a livello di singolo reparto).

Occorre descrivere come è costruito il codice, e come è strutturato e gestito il processo di pseudonimizzazione dei dati, cioè in quale fase dello studio si attua. Comunque, se si crea un elenco, e questohaunasualogica(ades.alfabeticaocronologica),nonèsufficientetoglierel'anagraficaedinserire ades.deicodiciprogressivi, occorrechesiano nonsequenzialierandomizzati(almenosel'estrazione dei dati è eseguibile una seconda volta con identici risultati). Insomma, il codice di pseudonimizzazione non può contenere elementi oggettivi – informativi o di carattere procedurale – che rendano possibile una identificazione dell'interessato a prescindere dalla chiave di pseudonimizzazione. Si può scrivere quanto segue:

> La pseudonimizzazione dei dati avverrà attraverso l'assegnazione di un codice. I dati personali sono trattati in associazione con questa informazione non direttamente identificativa, e la correlazione tra questa e i dati identificativi dell'interessato è conservata separatamente, accessibile al solo personale coinvolto nello studio, assicurandone, con idonee misure di sicurezza tecniche ed organizzative, la riservatezza. I codici di pseudonimizzazione sono costruiti secondo la seguente modalità: ……. I dati sono pseudonomizzati …. (*indicare in quale fase avvien la pseudonimizzazione dei dati*).

[17]Occorreprecisareseidati,inqualchemomentodelprocesso(es.trasferimentoocomunicazione,oppure archiviazione, sono cifrati, e con quale tecnica.

[18]Siricordache, peranonimizzazionecisiriferisceadunatecnicachesiapplicaaidatipersonalialfinedi ottenere una loro deidentificazione assoluta e irreversibile. In pratica, il dato anonimizzato non potrà più essere,innessuncontestoditrattamento,neppureinquellooriginario,ricollegatoall'interessato.Inpratica, 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).

Conquestipresupposti,ildatoanonimo/anonimizzatobenraramentepuòesserepresenteinunostudiose 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 modificadellaveridicitàdeidati,siricorreràatecnichedigeneralizzazione,consistononelgeneralizzaregli 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 raggruppamentoconalmenoKaltrepersone(K=valoredisoglia).Secondolaregoladellasoglia,lepersone 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 riferitononalsoloCaio,maancheaTizio,TazioeSempronio.Larelazionebiunivocatrailvaloreeduna (una sola) persona fisica viene così meno. Occorre indicare come si procede quando una tipologia di informazione resta sotto la soglia minima.

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

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

[21]Tralemisurecheostanoallaperdita,totaleoparziale,deidati,vièilbackup,chepuòesseresvoltocon una diversa frequenza. Si chiede di precisare se il backup dei dati è assicurato, e con quale tempistica.

[22]Ilterminemalwareindicaunprogrammacheèstatoprogettatoperdanneggiareuncomputer;èunasorta di genere ampio, rispetto alle specie quale troian , virus ecc.. Un virus è un malware che tende a danneggiare file e dati.

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

[24]Lamodalitàordinaria èlamessa adisposizionedell'interessatodell'informativaredattaaisensi dell'art, 13delRegolamento.

[25]Qualoranonsiapossibileoopportunoinformaregliinteressatiedacquisirneilconsensooccorrenonsolo attestarne ma documentarne e comprovarne i motivi tra i seguenti:

- ✓ motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione e l'informativa comporterebbe la rivelazione di notizie la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi;
- ✓ motivi di impossibilità organizzativa, nel senso che gli interessati, all'esito di ogni ragionevole sforzo compiutopercontattarli(ancheattraversolaverificadellostatoinvita,laconsultazionedeidatiriportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizionedeidatidicontattopressol'anagrafedegliassistitiodellapopolazioneresidente)risultino esserealmomentodell'arruolamentonellostudiodecedutiocomunquenoncontattabili,elamancata considerazionedeidatiriferitiaquesti,rispettoalnumerocomplessivodeisoggettichesiintende

coinvolgerenellaricerca,produrrebbeconseguenzesignificativeperlostudiointerminidialterazione dei relativi risultati (avuto riguardo ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento,allanumerositàstatisticadelcampioneprescelto,nonchéalperiododitempotrascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti).

Alcuniesempi:

- irreperibilità e/o oggettiva impossibilità organizzativa dovuta alla limitata disponibilità di indirizzi completi ed aggiornati dei pazienti;
- irreperibilitàe/ooggettivaimpossibilitàorganizzativadovutaall'elevatapercentualedipazientinonpiù seguiti dal centro (di sperimentazione coinvolto);
- irreperibilità e/o oggettiva impossibilità organizzativa dovuta all'elevato intervallo di tempo tra il primo accesso del paziente al centro (di sperimentazione coinvolto) ed il data entry dello Studio;
- impossibilità organizzativa e/o di fatto dovuta alla lontananza geografica dei pazienti che rende eccessivamente difficoltoso e costoso il loro ritorno al centro (di sperimentazione coinvolto) per le procedure di consenso, unitamente alla difficoltà di interagire con l'ausilio di strumenti elettronici da parte di pazienti anziani o aventi poca dimestichezza con le attrezzature elettroniche/informatiche;
- decessodelpaziente;
- intervenutaincapacitàdiintenderee/divoleredovutaall'aggravarsidellostatoclinico;
- sforzo oggettivamente sproporzionato rispetto agli obiettivi dello Studio che rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

Comunque, nel casoin cuiinformare gli interessati risulti impossibile o implichiuno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, occorre documentare le valutazioni effettuate e le evidenze raccolte per sostenere ciò, anche con riferimento a dati statistici (ad es. circa la mortalità della patologia oggetto dello studio) e, se del caso, i tentatividicontattoeffettuatiediloroesitipercentualisultotaledeipazientiarruolabili,oppurel'impegnodi risorsemateriali edumane che, inriferimentoalnumerodeipazientidacontattare, rendel'operazione non sostenibile dal punto di vista organizzativo. Occorre inoltre predisporre una informativa ex art. 14 del Regolamento, articolo che riguarda appunto le informazioni da mettere a disposizione dei pazienti non contattabili(nelcasodeidefunti,deiloroaventicausa)comeprevistodall'art.6delleRegoledeontologiche pertrattamentiafinistatisticiodiricercascientifica…;l'informativasaràpubblicatainunasezionededicata delsitoistituzionalepertuttaladuratadellostudiostesso(nelcasodipazientidefunti,abeneficiodifamiliari ecc.). Nell'informativa occorre indicare il soggetto cui sarà possibile rivolgersi, nel Centro di sperimentazione, per far valere i diritti degli interessati; si indica ordinariamente il responsabile aziendale della protezione dei dati, rpd@aou-careggi.toscana.it , 3666823917.

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

[27]E'Responsabile del trattamentoil soggettoesternorispetto altitolareche trattadatiperconto –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 materiadisciplinataeladuratadeltrattamento,lanaturaelafinalitàdeltrattamento,iltipodidatipersonali elecategoriediinteressati,gliobblighieidirittideltitolaredeltrattamento;taleattodeveessereredattoin modo tale che il responsabile tratti i dati personali soltanto su istruzione documentata del titolare del trattamento.

[28] Laparteconclusivadella DPIA,dopoladescrizione deltrattamentoe delle misuretecnico-organizzative individuate a garanzia della sua adeguatezza, è quella propriamente dedicata alla valutazione circa la sostenibilità dei rischi individuati. Tali rischi si articolano in riferimento alla perdita:

- diriservatezzadeidati
- diintegritàdeidati
- didisponibilitàdeidati

Lastimaconclusivadellaprobabilitàegravitàdiognitipologiadirischioèdaindicarsineiseguentitermini:

- indefinita
- trascurabile
- limitata
- importante
- massima.

Ognivalutazionesinteticadeveessereadeguatamentemotivata.

QualorasiutilizziREDCAP;èpossibilelimitarsiadindicarequantosegue:

Accessoillegittimoaidati
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 veicolate attraverso VPN.
Lecredenzialiamministrativesonoinpossessodelsolopersonaleinternoautorizzato.
Lecredenzialidigestionedell'applicativosonopersonalierilasciateaisolidipendentiautorizzatiche sono statiistruitiriguardolalorocorrettacustodia.

Modificheindesiderateaidati
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.

Perditadeidati
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.
Perglieventualidatalosscausatidaoperatoriinfedeli,valgonoleconsiderazionideipuntiprecedenti.