



Valutazione d'impatto sulla protezione dei dati

ai sensi dell'art. 35 Regolamento (UE) 2016/679 (RGPD)

	Nome e Cognome	Telefono	Email	Struttura organizzativa	Sede
Preposto al trattamento	Bruno Sposato	3382924035	Bruno.sposato@uslsudest.toscana.it	U.O.C. Pneumologia	P.O. della Misericordia di Grosseto

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

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

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

DESCRIZIONE DEL TRATTAMENTO DEI DATI

Denominazione del trattamento²

Long-term effectiveness of FF/UM/VI in COPD

Indicare le tipologie di dati oggetto del trattamento, specificando ogni tipologia di dato³

- *Data di nascita: fascia di età di 10 anni per soggetti a partire dai 40 anni (es. da 40 a 50 anni di età).*
- *Peso: fascia di BMI (<18,5 sottopeso; 18,5 – 24,9 normopeso; 25 – 29,9 sovrappeso; >30 obesità).*
- *Luogo di residenza: area geografica di pertinenza dell’Azienda Sanitaria Locale (saranno estratti i pazienti con residenza presso l’Azienda Sanitaria Toscana Sud Est senza specifiche della provincia).*
- *Presidio sanitario di cura: area geografica appartenente alla zona di pertinenza dello Sperimentatore.*
- *Data di ricovero: mese del ricovero senza specifica del giorno.*
- *Patologia espressa genericamente come ICD-9-CM nel livello minimo di specificità.*
- *Dati farmacologici: farmaci descritti in termini di principio attivo e relativa ATC; numero di pezzi e mese di erogazione senza specificare luogo di erogazione ed altri dati sensibili.*

Indicare le tipologie di interessati al trattamento⁴

FF/UM/VI con almeno 7 prescrizioni/anno del farmaco e che hanno avuto prescrizioni di LABA e/o LAMA o ICS/LABA nell’anno precedente l’inizio di FF/UM/VI, con età≥40 anni all’inizio dello studio.

Indicare i soggetti interni che partecipano al trattamento quali persone espressamente designate o autorizzate e se queste siano state adeguatamente istruite sul trattamento⁵

Lo sperimentatore principale ed i suoi collaboratori. Tutto il personale coinvolto nello studio è stato adeguatamente istruito sul trattamento dei dati.



Valutazione d'impatto sulla protezione dei dati

ai sensi dell'art. 35 Regolamento (UE) 2016/679 (RGPD)

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 trattamento⁶
Al momento del rilascio dell'autorizzazione aziendale all'avvio dello studio, saranno trasmesse le Istruzioni operative per il trattamento dei dati personali allo Sperimentatore Principale, in quanto individuato come Preposto al trattamento dei dati personali in riferimento alla conduzione del presente studio. Lo Sperimentatore Principale provvederà successivamente a nominare ed incaricare alcuni suoi collaboratori con profilo sanitario al trattamento dei dati, tramite una dichiarazione scritta e controfirmata che sarà conservata agli atti del fascicolo dello studio.

Descrivere il flusso dati (cioè come i dati sono spostati o elaborati). Occorre descrivere il flusso analiticamente nei suoi vari passaggi, operazioni, attori⁷

1. I dati di ciascun paziente vengono estrapolati dalla cartella clinica e/o da database amministrativi aziendali e pseudonimizzati, attribuendo a ciascun paziente un codice alfanumerico, randomizzato.
 2. Viene redatto dallo Sperimentatore Principale su un foglio elettronico di opencalc un elenco dei pazienti arruolati nello studio, a ciascuno dei quali corrisponde il proprio codice alfanumerico. Tale elenco viene archiviato in un pc aziendale protetto da password, nota solamente allo Sperimentatore Principale.
 3. Viene creata una cartella dedicata allo Studio nel cloud aziendale Alfresco, cui può accedere solamente lo Sperimentatore Principale e collaboratori da lui delegati, attraverso il proprio codice fiscale e la propria password.
 4. All'interno del cloud aziendale Alfresco, nella cartella dedicata allo Studio, viene generato un foglio di calcolo nel quale vengono trascritti tutti i dati pseudonimizzati dei pazienti arruolati, che costituisce la CRF elettronica dello studio.
 5. I dati dal foglio di calcolo vengo trascritti nel software di elaborazione dati STATA, in modo da poter procedere all'elaborazione statistica dei dati. I singoli dati raccolti vengono trascritti dallo Sperimentatore Principale, solo il codice pseudonimo che non riveste un'utilità nell'elaborazione statistica del dato, non verrà riportato nel software di elaborazione.
 6. I dati saranno resi anonimi irreversibilmente nella fase finale di pubblicazione in riviste scientifiche, provvedendo alla cancellazione definitiva ed irreversibile della corrispondenza tra il codice alfanumerico e l'identità del partecipante.
- Inoltre, sarà adottata la tecnica della generalizzazione, la quale consiste nel generalizzare gli attributi delle persone interessate modificando la rispettiva scala o ordine di grandezza (diluendo il livello di dettaglio di una determinata variabile).*

Nella fattispecie:

- *Data di nascita: fascia di età di superiore ai 40 anni compiuti.*
- *Luogo di residenza: area geografica di pertinenza dell'Azienda Sanitaria Locale (saranno estratti i pazienti con residenza presso l'Azienda Sanitaria Toscana Sud Est senza specifiche della provincia).*
- *Dati farmacologici: farmaci descritti in termini di principio attivo e relativa ATC; numero di pezzi prescritti all'anno.*
- *Dati clinici: valore ematiche dei globuli bianchi eosinofili espresso in eosinofili/mm³ di sangue.*

Tale tecnica è volta ad impedire l'individuazione di persone interessate mediante il loro raggruppamento con almeno "k" altre persone. A tale scopo, i valori degli attributi sono sottoposti a una generalizzazione tale da attribuire a ciascuna persona il medesimo valore. Come valore di soglia, si assume k uguale a 3 e, laddove tale valore non venisse raggiunto, i dati saranno cancellati.

Indicare dove vengono archiviati e conservati i dati⁸

Per quanto riguarda il file contenente l'elenco dei pazienti con il rispettivo codice alfanumerico, questo sarà archiviato presso un pc aziendale protetto da password, nota solamente allo Sperimentatore Principale.



Valutazione d'impatto sulla protezione dei dati

ai sensi dell'art. 35 Regolamento (UE) 2016/679 (RGPD)

Infine, il foglio elettronico di calcolo contenente i dati pseudonimizzati sarà conservato all'interno della cartella dedicata allo studio nel cloud aziendale Alfresco, cui può accedere solamente lo Sperimentatore Principale e collaboratori da lui delegati, attraverso il proprio codice fiscale e la propria password.

PRINCIPI FONDAMENTALI

PROPORZIONALITA' E NECESSITA'

Limitazione delle finalità: indicare la finalità del trattamento⁹

L'obiettivo del presente lavoro e quello di definire per il campione oggetto di studio, il numero di confezioni di corticosteroidi orali, antibiotici, salbutamolo; il numero di accessi in pronto soccorso/ricoveri ospedalieri; i livelli della funzione polmonare (spirometria) dei in particolare FEV1, osservati l'anno precedente (con LABA e/o LAMA o ICS/LABA) e durante i vari anni di terapia con FF/UM/VI.

Base giuridica: esplicitare le basi legali che rendono lecito il trattamento¹⁰

Ai sensi del Provvedimento del Garante Privacy del 09 Maggio 2024, richiamato l'art. 110, il Promotore dichiara che nel caso di specie non è possibile acquisire il consenso informato degli interessati per motivi di impossibilità organizzativa a causa della elevata numerosità del campione (circa 2000 soggetti) e la mancata raccolta dei dati riferiti al numero di interessati che non è possibile contattare, rispetto al numero complessivo dei soggetti che si intende arruolare nella ricerca, produrrebbe conseguenze significative per lo studio in termini di qualità dei risultati della stessa.

Si fa presente inoltre che i dati personali dei pazienti arruolati, in forma pseudonimizzata, potrebbero essere trattati ai fini della Farmacovigilanza, ai sensi della Direttiva 2010/84/UE e del Decreto MinSal del 30 Aprile 2015.

Se, durante l'estrazione dei dati dalle cartelle cliniche oppure dai database aziendali, lo Sperimentatore principale rilevasse reazioni avverse a farmaci assunti dai pazienti in studio, che non sono state segnalate al momento opportuno, deve provvedere a compilare il modulo per la segnalazione dell'ADR (Adverse Drug Reaction) ed inviarlo immediatamente al referente aziendale di farmacovigilanza, affinché provveda al suo inserimento nella Rete nazionale di Farmacovigilanza.

Minimizzazione dei dati: indicare i criteri utilizzati per garantire l'adeguatezza, la pertinenza e la non eccedenza dei dati utilizzati¹¹

I dati raccolti saranno quelli indispensabili alla esecuzione dello studio.

Limitazione della conservazione: indicare per quanto tempo sono conservati i dati e i criteri per la conservazione dei dati¹²

I dati saranno conservati per un periodo non superiore a quello necessario per le finalità dello studio per i quali sono stati raccolti, ovvero per tre anni dalla conclusione dello studio. La lista di decodifica (che associa codice univoco e nominativo del paziente) sarà eliminata al momento della fase finale di pubblicazione dell'articolo in riviste scientifiche. Anche il database informativo contenente i dati pseudonimizzati sarà conservato per un periodo massimo di tre anni dalla conclusione dello studio. Qualsiasi dato personale sarà eliminato dopo la scadenza del periodo di conservazione applicabile.

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 trattati¹³

I dati saranno revisionati dallo sperimentatore principale e dal suo team.

Durante ogni fase di manipolazione e di trasferimento dei dati (dalle fonti dei dati al foglio di calcolo elettronico al software statistico), è previsto un doppio controllo che sarà effettuato dallo sperimentatore principale.



Valutazione d'impatto sulla protezione dei dati

ai sensi dell'art. 35 Regolamento (UE) 2016/679 (RGPD)

Indicare se i dati sono trasferiti (si/no) ed eventualmente dove¹⁴

I dati personali dei pazienti arruolati nello studio verranno trasferiti dalle cartelle cliniche e dai database elettronici aziendali al file elettronico di calcolo.

I dati saranno successivamente trasferiti nel software di elaborazione dati STATA.

I dati saranno poi resi anonimi irreversibilmente nella fase finale di pubblicazione in riviste scientifiche, non solo provvederemo alla cancellazione definitiva ed irreversibile della corrispondenza tra il codice alfanumerico e l'identità del partecipante. Ma, non rappresentando essa stessa condizione sufficiente all'anonimizzazione dei dati, sarà, a tal scopo, adottata la tecnica della generalizzazione, la quale consiste nel generalizzare gli attributi delle persone interessate modificando la rispettiva scala o ordine di grandezza (diluendo il livello di dettaglio di una determinata variabile).

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Indicare come sono informati gli interessati al trattamento oppure, in alternativa, le ragioni per cui non è possibile informare gli interessati, specificando i dati di contatto del soggetto al quale gli interessati (o altri soggetti legittimati) possono indirizzare le proprie richieste relative all'esercizio dei diritti di accesso, , dei diritti di rettifica e di cancellazione, dei diritti di limitazione e di opposizione¹⁵

Gli interessati potranno visionare l'informativa predisposta per lo studio nel sito aziendale.

L'informativa è stata redatta ai sensi dell'art. 14 RGPD ed è rivolta ai soggetti non contattabili (anche deceduti).

La stessa, nel rispetto dell'art. 6 comma 3, delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica (provvedimento Garante n. 515 del 19 dicembre 2018) sarà resa disponibile mediante pubblicazione sul sito istituzionale del Centro di sperimentazione per la durata dello studio stesso (<https://www.uslsudest.toscana.it/>)

Tale informativa è stata sottoposta al Comitato Etico di Area Vasta Sud Est, ai fini dell'espressione del parere.

Ove applicabile: indicare come è acquisito il consenso degli interessati

Non applicabile.

Per ragioni organizzative non è possibile acquisire il consenso informato, dal momento che:

- lo Studio è no-profit e sarà svolto da professionisti sanitari dell'Azienda Sanitaria Toscana Sud Est;*
- e prevista l'analisi dei dati di un campione di circa 2000 soggetti;*
- recuperare il numero di telefono e/o l'indirizzo e-mail di ogni soggetto e contattarlo, richiederebbe un tempo medio di 10 minuti;*
- complessivamente, sarebbero necessari fino a 14 giorni, solamente per ricontattare tutti i soggetti;*
- questo periodo di tempo è inconciliabile con il tempo a disposizione dei professionisti sanitari coinvolti nel progetto di ricerca.*

Ai sensi del Provvedimento del Garante Privacy del 09 Maggio 2024, richiamato l'art. 110, il Promotore dichiara che nel caso di specie non è possibile acquisire il consenso informato degli interessati per motivi di impossibilità organizzativa a causa della elevata numerosità del campione pari a circa 2000 soggetti e la mancata raccolta dei dati riferiti al numero di interessati che non è possibile contattare, rispetto al numero complessivo dei soggetti che si intende arruolare nella ricerca, produrrebbe conseguenze significative per lo studio in termini di qualità dei risultati della stessa.

Ove applicabile: indicare se gli obblighi del responsabile del trattamento sono chiaramente definiti e formalizzati, e in caso di risposta positiva precisare come¹⁶

Non applicabile.

Valutare se, in caso di trasferimento dei dati al di fuori della UE, i dati godono di una protezione equivalente¹⁷

I dati non saranno trasferiti al di fuori dell'UE.



Valutazione d'impatto sulla protezione dei dati

ai sensi dell'art. 35 Regolamento (UE) 2016/679 (RGPD)

RISCHI

MISURE ESISTENTI O PIANIFICATE

indicare le misure tecniche ed organizzative adottate per garantire la sicurezza dei dati rispetto a trattamenti non autorizzati o illeciti, perdita, distruzione o danni accidentali¹⁸

Per quanto riguarda il file elettronico contenente i dati pseudonimizzati dei pazienti, sarà conservato all'interno di una cartella dedicata allo studio creata dallo Sperimentatore principale nel cloud aziendale Alfresco, cui potrà accedere solamente lo Sperimentatore Principale ed i collaboratori da lui incaricati al trattamento dei dati personali, attraverso il proprio codice fiscale e la propria password.

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono pseudonimizzati, e secondo quali modalità¹⁹

Il Centro presso il quale viene effettuato lo studio attribuirà ad ogni paziente un codice identificativo, al momento del suo coinvolgimento nello studio. Lo Sperimentatore principale del Centro presso il quale sarà effettuato lo studio sarà l'unico ed esclusivo soggetto a poter associare il codice identificativo ai rispettivi dati personali. Inoltre, tale codice sarà conservato in un file elettronico archiviato in un pc aziendale, presso apposito locale del centro sperimentale, protetto da password, nota solamente allo Sperimentatore Principale. Tale codice sarà accessibile solo allo Sperimentatore principale od altro collaboratore da questi incaricato al trattamento dei dati personali, quando indispensabile ai fini dello studio e per periodi di tempo limitati (per es., durante le attività di monitoraggio e verifica).

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono crittografati, e secondo quali modalità (ovvero quale sistema di crittografia è utilizzato)²⁰

I dati non verranno crittografati.

Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono anonimizzati, e secondo quali modalità/tecnica²¹

I dati saranno resi anonimi irreversibilmente nella fase finale di pubblicazione in riviste scientifiche, non solo provvederemo alla cancellazione definitiva ed irreversibile della corrispondenza tra il codice alfanumerico e l'identità del partecipante. Ma, non rappresentando essa stessa condizione sufficiente all'anonimizzazione dei dati, sarà, a tal scopo, adottata la tecnica della generalizzazione, la quale consiste nel generalizzare gli attributi delle persone interessate modificando la rispettiva scala o ordine di grandezza (diluendo il livello di dettaglio di una determinata variabile).

Nella fattispecie:

- *Data di nascita: fascia di età di 10 anni per soggetti a partire dai 18 anni (es. da 18 a 28 anni di età).*
- *Peso: fascia di BMI (<18,5 sottopeso; 18,5 – 24,9 normopeso; 25 – 29,9 sovrappeso; >30 obesità).*
- *Luogo di residenza: area geografica di pertinenza dell'Azienda Sanitaria Locale (saranno estratti i pazienti con residenza presso l'Azienda Sanitaria Toscana Sud Est senza specifiche della provincia).*
- *Presidio sanitario di cura: area geografica appartenente alla zona di pertinenza dello Sperimentatore.*
- *Data di ricovero: mese del ricovero senza specifica del giorno.*
- *Patologia espressa genericamente come ICD-9-CM nel livello minimo di specificità.*
- *Dati farmacologici: farmaci descritti in termini di principio attivo e relativa ATC; numero di pezzi e mese di erogazione senza specificare luogo di erogazione ed altri dati sensibili.*

Tale tecnica è volta ad impedire l'individuazione di persone interessate mediante il loro raggruppamento con almeno "k" altre persone. A tale scopo, i valori degli attributi sono sottoposti a una generalizzazione tale da



Valutazione d'impatto sulla protezione dei dati

ai sensi dell'art. 35 Regolamento (UE) 2016/679 (RGPD)

attribuire a ciascuna persona il medesimo valore. Come valore di soglia, si assume k uguale a 3 e, laddove tale valore non venisse raggiunto, i dati saranno cancellati."

Indicare se i dati sono soggetti a partizione²²

All'interno di questo centro sperimentale i dati non saranno soggetti a partizione.

Indicare con quali misure e cautele viene effettuato il trasferimento dei dati²³

I dati personali dei pazienti arruolati nello studio verranno trasferiti dalle cartelle cliniche e dai database elettronici aziendali al file elettronico di calcolo all'interno del cloud aziendale Alfresco.

I dati saranno poi trasferiti nel software di elaborazione dati STATA. I dati verranno poi anonimizzati, ai fini della divulgazione dei risultati dello Studio.

Indicare le procedure di gestione e controllo degli accessi logici ai sistemi (autenticazione) e se gli accessi sono tracciati²⁴

Per quanto riguarda invece i dati conservati nel file elettronico di calcolo, questo sarà archiviato in una cartella dedicata allo studio nel cloud aziendale Alfresco, cui è possibile accedere solamente con proprio codice fiscale e password personale, e che sarà accessibile solamente allo Sperimentatore principale ed a eventuali suoi collaboratori opportunamente incaricati a trattare i dati personali dei pazienti arruolati.

I documenti che sono caricati sul sito Alfresco sono responsabilità a livello privacy del manager dello stesso che autorizza la visualizzazione dei dati caricati su di esso ai collaboratori che ritiene che abbiano il diritto di visualizzare le informazioni.

Il programma Alfresco consente inoltre il tracciamento degli accessi degli utenti e degli amministratori e della cronologia di tutte le correzioni, le modifiche e le cancellazioni apportate ai dati.

Indicare i criteri gestione e controllo dell'accesso ai dati (profilazione)²⁵

Al momento del rilascio dell'autorizzazione aziendale all'avvio dello studio, saranno trasmesse le Istruzioni operative per il trattamento dei dati personali allo Sperimentatore Principale, in quanto individuato come Preposto al trattamento dei dati personali in riferimento alla conduzione del presente studio.

Lo Sperimentatore Principale provvederà successivamente a nominare ed incaricare alcuni suoi collaboratori con profilo sanitario al trattamento dei dati, tramite una dichiarazione scritta che sarà conservata agli atti del fascicolo dello studio.

Indicare le modalità di gestione e controllo degli accessi fisici

L'accesso fisico ai locali del centro di sperimentazione dove sono conservati i dati dei pazienti arruolati è vincolato al possesso delle chiavi dei locali, all'interno del reparto, dove è presente il pc aziendale in cui è conservata il file contenente l'elenco dei pazienti con il rispettivo codice alfanumerico. La disponibilità delle chiavi di accesso è sotto la responsabilità del Dirigente Medico Sperimentatore Principale.

Per quanto riguarda la protezione del foglio di calcolo contenente i dati pseudonimizzati dei pazienti, sarà garantita dal vincolo di accesso alla cartella dedicata allo studio all'interno del cloud aziendale Alfresco, cui può accedere solamente il Promotore/lo Sperimentatore principale ed il personale da questi formalmente autorizzato.

I documenti che sono caricati sul sito Alfresco sono responsabilità a livello privacy del manager dello stesso che autorizza la visualizzazione dei dati caricati su di esso ai collaboratori che ritiene che abbiano il diritto di visualizzare le informazioni.

Il programma Alfresco consente inoltre il tracciamento degli accessi degli utenti e degli amministratori e della cronologia di tutte le correzioni, le modifiche e le cancellazioni apportate ai dati.

Indicare con quale frequenza viene effettuato il backup dei dati ed il sistema utilizzato²⁶



Valutazione d'impatto sulla protezione dei dati

ai sensi dell'art. 35 Regolamento (UE) 2016/679 (RGPD)

Il backup dei dati viene assicurato giornalmente per il cloud Alfresco.

Indicare se il sistema prevede misure contro virus e malware²⁷
Tutti i pc aziendali sono tutelati da virus e malware da apposito sistema antivirus.

Indicare se i dati sono trattati anche su supporti cartacei, e come questi sono gestiti²⁸
Non applicabile.

Indicare le misure di sicurezza per la gestione delle postazioni di lavoro
All'interno del centro sperimentale, trattandosi di un presidio ospedaliero, sono presenti sistemi di sicurezza quali sistemi antincendio, vigilantes, telecamere, ingresso degli utenti controllato dal personale dedicato.

ACCESSO ILLEGITTIMO AI DATI (perdita di riservatezza)

Indicare le principali minacce che potrebbero concretizzare il rischio
Malfunctionamento software, Presa visione abusiva di dati, Uso non autorizzato di apparecchiature, Hackers che abbiano accesso al server di Alfresco.

Indicare le principali fonti di rischio
Un dipendente o un soggetto esterno malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, Incendio, Interruzione energia elettrica, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere alle informazioni.

Indicare le misure, tra quelle individuate, che contribuiscono a ridurre i rischi
*All'interno del presidio ospedaliero, sono presenti sistemi di sicurezza quali vigilantes, telecamere, ingresso degli utenti controllato dal personale dedicato.
 Inoltre, per poter accedere al locale in cui è presente il pc contenente l'elenco dei pazienti con il rispettivo codice alfanumerico, occorre disporre della chiave di accesso, che viene gestita dallo Sperimentatore Principale.
 Per quanto riguarda i dati conservati nel file elettronico, si fa presente che in tutti i pc aziendali è presente un sistema antivirus aggiornato che protegge dall'accesso illegittimo ai dati.
 Inoltre, la pseudonimizzazione dei dati rende difficile l'identificazione dei soggetti.
 Per quanto riguarda la protezione del foglio di calcolo contenente i dati pseudonimizzati dei pazienti, sarà garantita dal vincolo di accesso alla cartella dedicata allo studio all'interno del cloud aziendale Alfresco, cui può accedere solamente il Promotore/lo Sperimentatore principale ed il personale da questi formalmente autorizzato.
 I documenti che sono caricati sul sito Alfresco sono responsabilità a livello privacy del manager dello stesso che autorizza la visualizzazione dei dati caricati su di esso ai collaboratori che ritiene che abbiano il diritto di visualizzare le informazioni.
 Il programma Alfresco consente inoltre il tracciamento degli accessi degli utenti e degli amministratori e della cronologia di tutte le correzioni, le modifiche e le cancellazioni apportate ai dati.*

Indicare e argomentare una stima del livello di rischio, in relazione alla possibilità che la minaccia si concretizzi (probabilità) e alla valutazione delle conseguenze ove effettivamente si concretizzi (impatto), anche alla luce delle misure esistenti/pianificate (trascurabile, limitato, grave, massimo)
Alla luce delle misure adottate per minimizzare il rischio, come sopra indicate, la possibilità che il rischio si



Valutazione d'impatto sulla protezione dei dati

ai sensi dell'art. 35 Regolamento (UE) 2016/679 (RGPD)

concretizzi e trascurabile.

MODIFICHE INDESIDERATE DEI DATI (perdita di integrità)

Indicare le principali minacce che potrebbero concretizzare il rischio

Hackers che abbiano accesso al server di Alfresco, Errore nell'inserimento dei dati.

Indicare le principali fonti di rischio

Una terza parte autorizzata che sfrutta i privilegi di accesso per accedere alle informazioni, un dipendente o un soggetto esterno malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole.

Indicare le misure, tra quelle individuate, che contribuiscono a ridurre i rischi

All'interno del presidio ospedaliero, sono presenti sistemi di sicurezza quali vigilantes, telecamere, ingresso degli utenti controllato dal personale dedicato.

Inoltre, per poter accedere al locale in cui è presente il pc contenente l'elenco dei pazienti con il rispettivo codice alfanumerico, occorre disporre della chiave di accesso, che viene gestita dallo Sperimentatore Principale.

Durante ogni fase di trasferimento dei dati, è previsto un doppio controllo dell'operazione svolta.

Per quanto riguarda i dati conservati nel file elettronico, si fa presente che in tutti i pc aziendali è presente un sistema antivirus aggiornato che protegge dall'accesso illegittimo ai dati.

Inoltre, Alfresco permette il tracciamento di tutti gli accessi degli utenti e della cronologia di tutte le modifiche eventualmente apportate ai documenti in archivio.

Indicare e argomentare una stima del livello di rischio, in relazione alla possibilità che la minaccia si concretizzi (probabilità) e alla valutazione delle conseguenze ove effettivamente si concretizzi (impatto), anche alla luce delle misure esistenti/pianificate (trascurabile, limitato, grave, massimo)

Alla luce delle misure adottate per minimizzare il rischio, come sopra indicate, la possibilità che il rischio si concretizzi è trascurabile.

PERDITA, FURTO, CANCELLAZIONE NON AUTORIZZATA DEI DATI (perdita di disponibilità)

Indicare le principali minacce che potrebbero concretizzare il rischio

Hackers che abbiano accesso al server di Alfresco, Uso non autorizzato di apparecchiature, Malfunzionamento Software.

Indicare le principali fonti di rischio

Incendio, Interruzione energia elettrica, un dipendente o un soggetto esterno malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere alle informazioni.

Indicare le misure, tra quelle individuate, che contribuiscono a ridurre i rischi



Valutazione d'impatto sulla protezione dei dati

ai sensi dell'art. 35 Regolamento (UE) 2016/679 (RGPD)

Lo sperimentatore Principale, per ridurre il rischio accidentale di perdita dei dati, garantisce che giornalmente verifica che l'archivio elettronico sia completo di tutte le CRF sino a quel momento compilate ed al salvataggio dei dati conservati nel foglio elettronico archiviato all'interno della cartella dedicata allo studio nel cloud aziendale Alfresco.

All'interno del presidio ospedaliero, sono presenti sistemi di sicurezza quali vigilantes, telecamere, ingresso degli utenti controllato dal personale dedicato. Inoltre, per poter accedere al locale in cui sono conservati i dati dei pazienti, occorre disporre della chiave di accesso, che viene gestita dallo Sperimentatore Principale.

Per quanto riguarda i dati conservati nel file elettronico, si fa presente che in tutti i pc aziendali è presente un sistema antivirus aggiornato che protegge dall'accesso illegittimo ai dati.

Inoltre, Alfresco permette il tracciamento di tutti gli accessi degli utenti e della cronologia di tutte le modifiche eventualmente apportate ai documenti in archivio.

Indicare e argomentare una stima del livello di rischio, in relazione alla possibilità che la minaccia si concretizzi (probabilità) e alla valutazione delle conseguenze ove effettivamente si concretizzi (impatto), anche alla luce delle misure esistenti / pianificate (livello trascurabile, limitato, grave, massimo)

Alla luce delle misure adottate per minimizzare il rischio, come sopra indicate, la possibilità che il rischio si concretizzi è trascurabile.

PIANO D'AZIONE (misure da implementare , se valutato necessario, per migliorare la sicurezza del trattamento e mitigare ulteriormente il rischio)

Non sono state individuate misure possibili per mitigare ulteriormente il rischio.

Si allegano i seguenti documenti:

- 1) Protocollo di Studio, versione 1.0 del 16/03/2025
- 2) Informativa redatta ai sensi dell'art. 14 RGPD

VALUTAZIONE DEL PREPOSTO AL TRATTAMENTO (vedi nota 1)


(nome/cognome)

.....

.....

.....

.

	<p><i>Data</i> 08/09/2025</p>
<p>FIRMA</p>	

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

L'art. 2-quaterdecies del D.Lgs. 30 giugno 2003 n. 196 prevede che, tra le persone autorizzate al trattamento (cfr. nota 5), 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 ridenominata in Azienda (con delib. 332/2019) *Preposto*, termine che indica appunto un soggetto che sovrintende ad una data attività con ampio margine di autonomia gestionale e operativa anche rispetto alla specificità dei compiti e delle funzioni connessi al trattamento di dati.

2 Inserire titolo e codice dello studio.

3 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.

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

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

Per la persona espressamente designata, cfr. nota 1.

La persona autorizzata al trattamento è la persona fisica – dipendente o collaboratore - sottoposta, per quanto concerne il trattamento dei dati, al Titolare (cioè l'Azienda), e che tratta dati personali solo nella misura in cui sia stata a ciò autorizzata e istruita: le istruzioni delimitano l'ambito di trattamento autorizzato, e precisano le modalità secondo le quali il trattamento deve essere effettuato. Nessun incaricato può trattare dati senza adeguate istruzioni (che sono un suo diritto), e nessun incaricato, ricevutele, può effettuare operazioni di trattamento ulteriori rispetto a quelle da esse consentite. Tali istruzioni, nell'ottica della responsabilizzazione del titolare (che consiste nell'applicare i principi previsti all'art. 5 del regolamento UE 2016/679, documentandone le modalità di applicazione), devono essere raccolte in un atto di nomina a firma del P.I. (atto che potrà essere anche riferito al gruppo di sperimentazione nel suo complesso, oppure qualora i compiti, all'interno del gruppo di sperimentazione siano significativamente differenziati, essere più personalizzato e quindi nominativo).

6 Qui si può far riferimento:

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

tratta dati per conto – cioè per le finalità – del titolare, secondo le modalità da questo indicate. Ai sensi dell'art. 28 paragrafo 3 del Regolamento tale incarico deve essere formalizzato in un contratto o altro atto giuridico, che precisi la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento; tale atto deve poi essere tale che il responsabile tratti i dati personali soltanto su istruzione documentata del titolare del trattamento.

L'indicazione di tali soggetti deve, nella misura del possibile, ricomprendere la loro denominazione.

7 Un trattamento di dati personali si traduce in un flusso di informazioni, che può coinvolgere vari ambiti (es. banche dati), soggetti ecc., e che può sostanziarsi in una serie di operazioni (es. la raccolta dei dati, per la quale occorre indicare come essi vengono selezionati e trasmessi, ad es. in un foglio di raccolta o in un database; il trasferimento dei dati – il loro mero spostamento, anche all'interno di un singolo titolare – o la loro comunicazione, tra due o più titolari; le modalità di elaborazione ecc.).

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

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

In ordine ai profili di sicurezza, anche in relazione alla esattezza ed integrità dei dati, è utile precisare che un foglio excel su un pc in locale non soddisfa i requisiti minimi (la DPIA non otterrà il parere positivo del Responsabile della Protezione dei dati aziendale, tenuto conto delle ripetute valutazioni negative espresse dall'Autorità, in sede di autorizzazione a seguito di consultazione preventiva in vigenza dell'originaria formulazione dell'art.110 d.lgs 196/2003, in riferimento all'utilizzo di strumenti informatici di archiviazione dati che non assicurino la tracciabilità degli accessi e delle operazioni effettuate)

Il sistema di archiviazione e conservazione dei dati dello studio deve garantire il tracciamento degli accessi e delle operazioni effettuate, garanzie contro virus, malware ecc..

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

9 Finalità del trattamento vale il suo scopo pratico. Occorre dunque indicare, posto che il trattamento è ovviamente funzionale alla esecuzione dello studio, quali sono gli scopi che si intendono raggiungere con lo studio medesimo. Qualora i dati vengano raccolti per una finalità ulteriore (es. di cura, il che significa che saranno trattati anche con modalità identificativa), occorre integrare tale specifico elemento nell'informativa sul trattamento dei dati.

10 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 dal parere positivo del competente Comitato etico a livello territoriale, e dal rispetto delle garanzie previste dall'art. 110, comma 1, quarto capoverso, d.lgs 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali" quali individuate dal Garante nel provvedimento n. 298 del 9 maggio 2024 ovvero:

- *redazione e pubblicazione di una Valutazione d'impatto;*
- *trasmissione all'Autorità Garante del relativo link di pubblicazione*
- *esplicitazione puntuale e motivata nel protocollo di ricerca delle ragioni per cui non si ritiene possibile procedere alla raccolta del consenso*

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.

10

11 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). Tali requisiti sono da intendersi 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. Spetta al Titolare, nella logica della responsabilizzazione, valutare quali dati siano o meno necessari, esplicitando le relative motivazioni

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 (laddove si elencano appunto le informazioni che si ritiene necessario raccogliere per raggiungere gli obiettivi dello studio. E' di tale necessità che deve essere data brevemente evidenza, anche soltanto indicando in sintesi che "i dati raccolti sono quelli indispensabili alla esecuzione dello studio".

12 In riferimento agli studi osservazionali, un termine puntuale per la conservazione dei dati utilizzati non è previsto (tali studi non sono ricompresi nel Regolamento UE 536/2014, che per le sperimentazioni su farmaci e dispositivi estende la conservazione ad "almeno 25 anni") e , pertanto, quello scelto deve essere motivato. Il termine deve essere commisurato allo scopo principale della conservazione dei dati, che è anzitutto quello di rendere possibile verifiche o controlli della base dati dello studio successivamente alla pubblicazione Si consiglia di scrivere qualcosa di analogo a quanto segue:

Il termine di conservazione dei dati è fissato a ... (inserire il numero di anni ritenuto necessario) anni; si evidenzia la consapevolezza che, per gli studi osservazionali, la valenza normativa dei termini di conservazione previsti dalle disposizioni vigenti, sempre orientate a regolare gli studi interventistici, è, se non assente, comunque non direttamente ed immediatamente prescrittiva, così che viene comunque chiamata in causa la responsabilizzazione del Titolare.

Si è considerato opportuno applicare a questo studio osservazionale il termine di ... anni in quanto ...

Ove si utilizza il termine di prassi di 7 anni, la motivazione può essere resa come segue, sostituendo l'ultima frase:

Si è considerato opportuno applicare a questo studio osservazionale il termine di conservazione di 7 anni già previsto dal D.Lgs. 6 novembre 2007, n. 200, riferibile ad una prassi consolidata e soprattutto ritenuto sufficiente e non eccedente in relazione allo scopo di consentire eventuali controlli successivi sulla correttezza delle inferenze effettuate nella valutazione dei dati raccolti nel corso della ricerca. Il termine settennale è commisurato alla opportunità di conservare una base dati statistica per successive verifiche o richieste di precisazioni circa i risultati pubblicati.

Si ricorda che mediante l'informativa ex art. 13 o ex art. 14 del Regolamento occorre indicare e comunicare ai soggetti interessati, che:

- sono raccolti solo i dati strettamente necessari per il perseguimento delle finalità;
- decorsi i termini di conservazione, i dati personali saranno distrutti, cancellati o resi anonimi (descrivendo i meccanismi per la cancellazione o anonimizzazione dei dati).

Se i dati sono conservati a tempo indeterminato a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è necessario indicare le misure adottate per garantire il principio di minimizzazione.

13 In questo caso l'esattezza del dato non si intende riferita al suo aggiornamento, ma alle modalità con le quali i dati sono raccolti dalla documentazione originale e dunque duplicati, garantendone appunto l'esattezza rispetto a quella, per le finalità dello studio. Ovvio che misure di controllo sono meno necessarie quando l'estrazione da un data base informatico avviene quasi automaticamente a seguito dell'inserimento di dati parametri, rispetto alla copia manuale, per la quale occorre individuare una procedura di verifica e controllo.

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

Occorre indicare inoltre se i dati sono eventualmente trasferiti:

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

Il trasferimento dei dati (esclusi i dati genetici) all'interno dell'organizzazione del titolare/Azienda deve essere effettuato con modalità sicura, anche con strumenti di cooperazione applicativa oppure utilizzando strumenti di messaggistica che utilizzino canali di comunicazione protetti (ove si utilizzino la PEC o la posta ordinaria proteggendo l'allegato con tecniche di cifratura e rendendolo accessibile tramite una password per l'apertura del file trasmessa separatamente e con modalità diversa da quella utilizzata per la trasmissione dei dati. Per ogni trasferimento di dati genetici e per il trasferimento dei dati (diversi da quelli genetici) all'esterno dell'organizzazione del titolare/Azienda non è possibile utilizzare la mail ordinaria ma solo strumenti di cooperazione applicativa o di messaggistica che utilizzino canali di comunicazione protetti (ivi compresa la PEC), cifrando i dati e fornendo la chiave di decifrazione attraverso canali di comunicazione differenti da quelli utilizzati per la

trasmissione dei dati.

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

15 Si tratta di due distinte prescrizioni. Anzitutto, qualora non sia possibile o opportuno informare gli interessati e acquisirne il consenso occorre non solo attestarne ma documentarne e comprovarne i motivi tra i seguenti:

- motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione e l'informativa comporterebbe la rivelazione di notizie la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi;
- motivi di impossibilità organizzativa, nel senso che gli interessati, all'esito di ogni ragionevole sforzo compiuto per contattarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente) risultino essere al momento dell'arruolamento nello studio deceduti o comunque non contattabili, e la mancata considerazione dei dati riferiti a questi, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati (avuto riguardo ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti).

Alcuni esempi:

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

Comunque, nel caso in cui informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, occorre documentare nel presente documento (e obbligatoriamente nel Protocollo di studio, come prescritto dal Garante nel provv. n. 298 del 9 maggio 2024, che individua le garanzie di cui all'art. 110, comma 1, quarto capoverso, d.lgs 30 giugno 2003 n. 196 "*Codice in materia di protezione dei dati personali*") le valutazioni effettuate e le evidenze raccolte per sostenere ciò, anche con riferimento a dati statistici (ad es. circa la mortalità della patologia oggetto dello studio) e, se del caso, i tentativi di contatto

effettuati ed i loro esiti percentuali sul totale dei pazienti arruolabili, oppure l'impegno di risorse materiali ed umane che, in riferimento al numero dei pazienti da contattare, rende l'operazione non sostenibile dal punto di vista organizzativo.

Occorre inoltre fornire alcune informazioni e renderle disponibili, predisponendo per lo studio l'informativa ex art. 13 del Regolamento, da utilizzarsi quando gli interessati sono contattabili. Qualora non lo siano (anche nel caso di defunti) occorre predisporre una informativa ai sensi dell'art. 14 del Regolamento, che, nel rispetto dell'art. 6 comma 3, delle *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica* (provvedimento Garante n. 515 del 19 dicembre 2018) sarà resa disponibile mediante pubblicazione sul sito istituzionale del Centro di sperimentazione per la durata dello studio stesso (nel caso di pazienti defunti, a beneficio di familiari ecc.).

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

16 Per il Responsabile del trattamento cfr. nota 6.

17 Si pone qui nuovamente la questione del trasferimento dei dati extra UE (cfr. nota 14), 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.

18 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 la distruzione accidentale o non autorizzata di dati personali.

Occorre indicare, sinteticamente, le misure adottate da un punto di vista organizzativo, nonché quelle assicurate dal sistema sul quale i dati sono archiviati, anche attraverso il rimando alla relativa documentazione tecnica.

E' ovvio che la modifica, la perdita o la non accessibilità ai dati sono questioni che non attengono esclusivamente alla privacy, ma direttamente alla qualità del dato di ricerca.

19 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 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 parlante del del mero nome giuridico), ma neppure un codice che sia conosciuto al di fuori del gruppo di sperimentazione (es. il numero nosologico o simile, anche a livello di singolo reparto).

Occorre descrivere come è costruito il codice, e come è strutturato e gestito il processo di pseudonimizzazione dei dati, cioè in quale fase dello studio si attua.

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

La pseudonimizzazione dei dati avverrà attraverso l'assegnazione di un codice. I dati personali sono trattati in associazione con questa informazione non

direttamente identificativa, e la correlazione tra questa e i dati identificativi dell'interessato è conservata separatamente, accessibile al solo personale coinvolto nello studio, assicurandone, la riservatezza con le seguenti misure di sicurezza tecniche e organizzative:.....

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

21 Si ricorda che, per anonimizzazione ci si riferisce ad una tecnica che si applica ai dati personali al fine di ottenere una loro deidentificazione assoluta e irreversibile. In pratica, il dato anonimizzato non potrà più essere, in nessun contesto di trattamento, neppure in quello originario, ricollegato all'interessato. Va evidenziato che l'anonimizzazione non può considerarsi realizzata attraverso la mera rimozione delle generalità dell'interessato o sostituzione delle stesse con un codice pseudonimo. Si ribadisce che un set di dati privato dell'anagrafica non è 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 in prospettiva e tenuto conto di tutti i mezzi (economici, informazioni, risorse tecnologiche, competenze, tempo) nella disponibilità di chi (titolare o altro soggetto) provi a utilizzare tali strumenti per identificare un interessato, della possibilità di raccordo con la relativa anagrafica, nel senso che questa non è più recuperabile (e non è dunque più possibile una reidentificazione, cioè la eventualità che, partendo da dati erroneamente ritenuti anonimi, si riesca a recuperare informazioni identificative degli interessati, sia direttamente, sia tramite metodi di correlazione e deduzione).

Con questi presupposti, il dato anonimo/anonimizzato ben raramente può essere presente in uno studio se non nella fase conclusiva, quando si aggregano i dati in vista della pubblicazione degli esiti. La procedura con cui si anonimizzano i dati in vista della pubblicazione deve essere descritta; ordinariamente, non essendo auspicabile, in uno studio clinico il ricorso a tecniche di *randomizzazione*, che consistono nella modifica della veridicità dei dati, si ricorrerà a tecniche di *generalizzazione*, consistono nel generalizzare gli attributi delle persone interessate, diluendo i livelli di dettaglio. Si utilizzerà di solito, tra queste, il K-Anonimato, tecnica volta ad impedire l'individuazione di persone interessate mediante il loro raggruppamento con almeno K altre persone (K=valore di soglia). Secondo la regola della soglia, le persone cui si riferiscono i dati si considerano non identificabili se il loro numero è superiore ad un certo valore prestabilito (valore di soglia). Il valore minimo ordinariamente attribuibile alla soglia è pari a tre (ma nel valutare il valore della soglia si deve tenere conto del livello di sensibilità delle informazioni, e dell'effettivo rischio di danno ad esse correlato, per cui nel caso di studio clinico il valore è fissato a 4)). La regola della soglia sottende che il valore originale X possa essere riferito non al solo Caio, ma anche a Tizio, Tazio e Sempronio. La relazione biunivoca tra il valore X ed una (una sola) persona fisica viene così meno.

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

23 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.

24 Il tracciamento degli accessi, con finalità di sicurezza e controllo, può riguardare tanto operazioni che modificano la consistenza dei dati che la loro mera consultazione. Tale tracciamento si traduce nella conservazione di file di log, che sono conservati per un certo tempo. E' richiesto di specificare, appunto, se sono tracciati gli accessi degli utenti e degli amministratori, se sono tracciati anche gli accessi in consultazione, se sono tracciati i riferimenti temporali degli accessi, per quanto tempo gli eventuali file di log sono conservati. Il tracciamento degli accessi, con la registrazione delle operazioni effettuate, in particolare di modifica dei dati, pare essere una misura essenziale per garantire la sicurezza dei dati, ovvero

la loro esattezza ed integrità.

25 La profondità di accesso indica il *quantum* di accessibilità ai dati - tanto da un punto di vista quantitativo che di tipologia di informazioni - che è concesso ad una determinata persona autorizzata al trattamento ; a questa possono inoltre essere riconosciute particolari prerogative di intervento sui dati (lettura, scrittura, cancellazione, elaborazione ecc.). Tutte queste prerogative sono connesse ad uno o più profili di autorizzazione (e di correlato ambito di trattamento di dati), che si chiede - qualora differenziati - di descrivere in breve.

26 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.

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

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