VALUTAZIONE DI IMPATTO

Redatto:	Lunedì 1 dicembre 2025

Verificato:	DPO, …….

Approvato:	

Versione:	1.0

DATI DI CONTROLLO DEL DOCUMENTO

Storia del documento				
versione	data	capitolo/paragrafo	modifica apportata	motivo modifica
01	1/12/2025	---	Nessuna	Prima versione

INDICE

1. Informazioni generali

1.1 Titolare del trattamento

La presente DPIA è stata redatta dall'ASL TO5, in qualità di Titolare del trattamento ("Titolare del trattamento" o "ASL TO5").
Tale ruolo è assunto in quanto l'ASL TO5 è il promotore dello studio, avendone determinato finalità e mezzi di trattamento.
Il Principal Investigator (Responsabile dello studio) è il dott. Bergamo Daniele.

1.2 Contesto di riferimento

Oggetto della presente valutazione d'impatto (Data Protection Impact Assessment – DPIA) è il trattamento dei dati personali dei pazienti che hanno ricevuto prestazioni sanitarie nell'ambito delle attività di cura presso la S.C. Medicina Interna del Presidio Ospedaliero Santa Croce di Moncalieri dell'ASL TO5, al fine di condurre uno studio monocentrico, osservazionale, retrospettivo.

1.3 Standard di riferimento per la predisposizione della DPIA

La presente DPIA è stata realizzata utilizzando come base le informazioni contenute nel software sviluppato dall'Autorità francese per la protezione dei dati (CNIL), in conformità alle indicazioni fornite nelle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" (WP 248 rev. 01 e adottate dall'EDPB il 4 aprile 2017 e modificate il 4 ottobre 2017 – "***Linee Guida***").*
Inoltre, per la valutazione del rischio è stata utilizzata la metodologia dell'*European Union Agency For Network and Information Security* ("**ENISA**") descritta all'interno del documento "*Guidelines for SMEs on the security of personal data processing*" raggiungibile al seguente link https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing.

Sono stati, infine, tenuti in considerazione alcuni dei requisiti della norma ISO/IEC 29134 "*Information technology — Security techniques — Guidelines for privacy impact assessment":* in particolare, valutazione necessità DPIA (art. 6.2), composizione del DPIA team (art. 6.3.1), piano di trattamento del rischio residuo e revisione e verifica della DPIA (art. 6.5.3 – 6.5.4).

1.4 Descrizione del quadro normativo e regolatorio, standard e buone prassi

- Regolamento UE 679/2016 [cons. 33-50-52-53-62-65-113-156-157-159-160-161-162-163; artt. 5-9-14-17-21-89];
- D.Lgs. 196/2003 (mod. D.Lgs. 101/2018) [artt. 78-100-105-106-110-110 *bis*] "), come modificato da ultimo dall'art. 1, comma 1, della l. 29 aprile 2024, n. 56. di conversione del D.L. 2 marzo 2024, n. 19;
- Allegato A5 - Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018;
- Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR Versione 2.0 Adottate il 7 luglio 2021;
- Provvedimenti Autorità Garante [provv. GPDP 497/2018 riguardante le aut. gen. 9/2016 e aut. gen. 8/2016];

- Provvedimento del 14 gennaio 2021 - Regione Veneto. Codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica;
- Convenzione di Oviedo – "Convenzione per la protezione dei Diritti dell'Uomo e della dignità dell'essere umano nei confronti dell'applicazioni della biologia e della medicina: Convenzione sui Diritti dell'Uomo e la biomedicina", del 4 aprile 1997;
- GCP - ICH Harmonised Guideline – "Integrated Addendum to Ich E6(r1): Guideline For Good Clinical Practice", del 9 novembre 2016;
- EDPB – "Documento sulla risposta alla richiesta della Commissione europea di chiarimenti sull'applicazione coerente del GDPR, concentrandosi sulla ricerca sanitaria", adottato il 2 febbraio 2021;
- GPDP – Provvedimento del 9 maggio 2024, "Individuazione delle misure di garanzia ai sensi degli artt. 106, comma 2, lett. d) e 110 del Codice";
- GPDP – "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del D. Lgs. 10 agosto 2018, n. 101 – 19 dicembre 2018", pubblicate sulla G.U. n. 11 del 14 gennaio 2019;
- Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Tecniques, April 2014;
- ISO/IEC 20889:2018 - Privacy enhancing data de-identification terminology and classification of techniques;
- ISO 25237:2017 – Health informatics – Pseudonymization;
- ISO/IEC 27559:2022 - Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework;
- NIST - NISTIR 8053 De-Identification of Personal Information, October 2015;
- DICOM PS3:15 2016 – Annex E;
- NIST SP 800-188 De-Identifying Government Datasets: Techniques and Governance, September 2023;
- ENISA, "Data Pseudonymisation: Advanced Techniques & Use Cases Technical Analysis of Cybersecurity Measures iI Data Protection and Privacy", January 2021;
- ENISA, "Privacy Enhancing Technologies: Evolution and State of the Art", March 2017.

1.5 Procedura per la conduzione della DPIA

La presente DPIA si articola nelle seguenti fasi:

- Fase 0: Determinazione della necessità di condurre la DPIA e costituzione del team DPIA
- Fase 1: Descrizione del trattamento
- Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento
- Fase 3: Calcolo del rischio
- Fase 4: Misure di mitigazione del rischio adottate
- Fase 5: Consultazione degli interessati
- Fase 6: Calcolo del rischio residuo, piano di remediation e parere del DPO
- Fase 7: Eventuale consultazione dell'autorità garante per la protezione dei dati personali
- Fase 8: Monitoraggio e riesame nel tempo della DPIA ed eventuale aggiornamento

2. Fase 0: Determinazione della necessità di condurre la DPIA e costituzione del team DPIA

2.1 Necessità di svolgere la DPIA

Il Titolare del trattamento al fine di garantire che il trattamento dei dati relativi allo stato di salute dei pazienti arruolati nell'ambito dello studio sia svolto in conformità al Regolamento UE 2016/679 si impegna a rispettarne i principi fondamentali.

In particolare, si è provveduto a seguire i principi fondamentali relativi alla valutazione d'impatto sulla protezione dei dati di cui al Regolamento (UE) 2016/679 (di seguito GDPR) così come schematizzati nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" del 4 ottobre 2017 pubblicate dal Gruppo di lavoro Articolo 29 (WP29), e si è riscontrato che i trattamenti presi in considerazione possono presentare rischi elevati.

Il trattamento preso in esame, rispetto a quelli individuati nell'allegato 1 al provvedimento del Garante della protezione dei dati personali n. 467 dell'11 ottobre 2018, "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto", rientra nei:

- Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo) – (rif. 6);
- Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse – (rif. 10);

Preso atto che il sopracitato provvedimento asserisce che la valutazione d'impatto sulla protezione dei dati debba essere effettuata ogniqualvolta ricorra almeno un criterio in quanto è indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati, si è ritenuto opportuno procedere all'esecuzione della valutazione d'impatto.

Inoltre, l'art. 110 del Codice Privacy, a seguito della modifica operata dall'art. 1, comma 1, della l. 29 aprile 2024, n. 56. di conversione del D.L. 2 marzo 2024, n. 19 richiede la redazione di una valutazione di impatto, e il rispetto delle garanzie che saranno individuata dal Garante, ai sensi dell'articolo 106, comma 2, lettera d) del Codice Privacy, qualora non sia possibile acquisire il consenso degli interessati per gli studi clinici.

Data l'impossibilità di contattare tutti gli interessati e ottenere un valido consenso ai sensi dell'art. 9 del Reg. UE 679/2016, stante la necessità per conseguire i fini dello studio dell'inclusione di pazienti deceduti e non più contattabili, occorre procedere ai sensi dell'art. 110 del Codice Privacy.

2.2 Team di lavoro

Il presente documento è stato redatto da un team composto da:

- Dott. Daniele Bergamo: Sperimentatore principale
- Ing. Paolo Petrucci: Direttore S.C. Tecnologie Informatiche e Servizi Informativi;
- Dott.ssa Anna Cerrato: Ufficio privacy;

- Ing. Maurizio Pastore: DPO (per le impostazioni metodologiche e per il parere sulla DPIA stessa).

Il progetto di studio sarà sottoposto al competente Comitato Etico Indipendente per la richiesta di parere positivo.

2.3 Piano delle attività

Al termine della predisposizione della DPIA, il documento verrà sottoposto al parere del DPO.

Il team dovrà recepire almeno parzialmente le osservazioni del DPO, evidenziando eventuali scostamenti, per l'approvazione da parte del Legale Rappresentante.

Laddove il rischio residuo sia elevato, stante la modifica dell'art. 110 del Codice, sopra indicata, si procederà all'invio del documento all'Autorità ai sensi dell'art. 110 del Codice e dell'art. 36 del Regolamento.

A fronte di un parere positivo ma condizionato, il team dovrà recepire le osservazioni del Garante e ritornare il documento per l'approvazione finale.

3. Fase 1: Descrizione del trattamento

3.1.1 Il trattamento oggetto della Valutazione di Impatto

Si tratta di uno studio monocentrico, osservazionale, retrospettivo, condotto sui pazienti ricoverati presso la S.C. Medicina Interna dell'Ospedale Santa Croce di Moncalieri, ai quali, durante il ricovero, è stato effettuato lo screening per valutare la presenza di delirium tramite test 4AT e per i quali sono disponibili le informazioni cliniche necessarie al calcolo di uno score di predizione del rischio di sviluppare delirium elaborato da Zucchelli e colleghi nel 2021.

Lo studio comprende una sola fase retrospettiva, in quanto utilizza esclusivamente dati clinici già raccolti nell'ambito dell'attività assistenziale ordinaria tra gennaio e novembre 2024. Non è prevista alcuna fase prospettica né alcun arruolamento attivo di nuovi pazienti.

La fase retrospettiva consiste nella revisione sistematica e nell'estrazione dei dati clinici registrati nella cartella clinica relativi a 983 pazienti ricoverati nel periodo gennaio–novembre 2024, con successiva inclusione nel campione analitico di 679 pazienti, dopo esclusione di coloro che presentavano delirium al momento della dimissione dal Pronto Soccorso o all'ammissione in reparto (come previsto dal protocollo scientifico).
Non è previsto contatto diretto con i pazienti né somministrazione di questionari o interventi specifici: tutta la raccolta informativa utilizza **dati già disponibili**.

La raccolta dei dati verrà eseguita tramite software Microsoft Excel da pacchetto Office Professional versione 2021 installato su un pc dedicato, che sarà costantemente aggiornato tramite il sistema WSUS aziendale.

I dati verranno organizzati utilizzando tabelle, suddivise come di seguito precisato:

1. Tabella "Record paziente" [contiene dati potenzialmente identificativi (solo per la fase iniziale di estrazione)]:
   - cognome e nome;
   - età;
   - sesso;
   - data di ricovero e dimissione
2. Tabella "Informazioni cliniche e diagnostiche" (contiene esclusivamente dati sanitari utili allo studio):
   - punteggi giornalieri del test 4AT;
   - variabili necessarie al calcolo dello Zucchelli Score:
     - età >75 anni;
     - anamnesi di demenza;
     - deficit uditivo;
     - utilizzo di terapia psicotropa in cronico;
   - Charlson Comorbidity Index;
   - esiti clinici (durata degenza, esito alla dimissione);

Le tabelle saranno collegate per mezzo di un identificativo paziente random univoco (Codice alfanumerico costituito da 8 caratteri es: 6VHNOT#7)
La corrispondenza tra nominativo del paziente e il Codice univoco sarà registrata su file Excel separato.

Per quanto riguarda la fase retrospettiva, con riferimento ai dati personali già presenti nei sistemi del Titolare e raccolti in occasione delle prestazioni sanitarie, numerosi pazienti risultano deceduti o non reperibili, dato che il protocollo richiede la raccolta dati a partire dal 2012 (oltre 10 anni addietro). In tal senso, non essendo possibile informarli e raccoglierne il relativo consenso, il Titolare ritiene di procedere ai sensi dell'art. 110 del d.lgs. 196/2003.
In ogni caso, verrà fornita adeguata informativa tramite contatto con i pazienti rintracciabili e tramite pubblicazione sul sito web aziendale.
Eventualmente i pazienti non rintracciati potranno, anche per il tramite dei propri aventi causa ai sensi dell'art. 2-terdiecies del Codice Privacy, esercitare la revoca del consenso (anche se non materialmente prestato) tramite il cosiddetto opt-out.

Durata prevista del trattamento
Periodo di raccolta dati: gennaio – novembre 2024 (già concluso).
Periodo di analisi: limitato al tempo necessario al completamento dello studio, alla valutazione statistica e alle eventuali revisioni editoriali.
Durata conservazione dati pseudonimizzati: tempo strettamente necessario alla validazione scientifica, secondo policy aziendale.

Finalità dello studio
L'obiettivo principale dello studio osservazionale no-profit è validare lo score elaborato da Zucchelli e colleghi nel 2021 in una coorte di pazienti ricoverati in Medicina Interna, valutandone la capacità predittiva (AUC, sensibilità, specificità, calibrazione) e la potenziale utilità clinica nella stratificazione precoce del rischio di delirium.

Gli endpoint considerati includono:
- incidenza del delirium durante il ricovero;
- prevalenza dei fattori di rischio che compongono lo score;
- performance diagnostica del punteggio dello score (AUC, PPV, NPV);
- associazione tra score e outcome clinici (mortalità, dimissione presso struttura residenziale, durata della degenza).

Potenziali benefici derivanti dalla sperimentazione allo studio:

I potenziali benefici attesi dallo studio sono molteplici e riguardano sia la pratica clinica sia la gestione dei pazienti ricoverati in Medicina Interna.

1. Miglioramento dell'identificazione precoce dei pazienti a rischio di delirium
La validazione dello score in un contesto di Medicina Interna permette di:
- riconoscere tempestivamente i pazienti con elevata probabilità di sviluppare delirium durante il ricovero;
- agevolare l'attivazione precoce di interventi preventivi non farmacologici, riconosciuti come misura più efficace nella riduzione dell'incidenza e della durata del delirium;
- migliorare la stratificazione del rischio nelle prime ore dall'ingresso, utilizzando informazioni semplici e immediatamente disponibili.

2. Ottimizzazione della gestione clinico-assistenziale
Il delirium è associato a esiti negativi quali prolungamento della degenza, complicanze, istituzionalizzazione e aumento della mortalità. Lo studio può contribuire a:
- ridurre gli episodi di delirium attraverso protocolli di prevenzione personalizzati;
- orientare il personale sanitario verso un monitoraggio più mirato dei soggetti ad alto rischio;

- diminuire l'utilizzo improprio di farmaci antipsicotici, di cui non è dimostrata l'efficacia preventiva.

3. Razionalizzazione delle risorse ospedaliere
Un sistema affidabile di stratificazione del rischio consente:
- una più efficiente allocazione delle risorse assistenziali;
- la riduzione di degenze evitabili dovute a delirium;
- la diminuzione di trasferimenti non necessari in reparti ad alta intensità di cura legati a complicanze del delirium.

4. Avanzamento delle conoscenze scientifiche
Lo studio, applicato per la prima volta in un reparto di Medicina Interna, produce:
- nuove evidenze sull'affidabilità del *Zucchelli Delirium Risk Score* in un setting diverso da quello di sviluppo (Pronto Soccorso);
- dati qualitativi e quantitativi sulla popolazione anziana ricoverata in Medicina Interna;
- contributi rilevanti alla letteratura scientifica e potenziale base per studi multicentrici futuri.

5. Benefici indiretti per i pazienti e la comunità
L'applicazione di strumenti predittivi validati:
- migliora la qualità dell'assistenza e riduce complicanze evitabili;
- contribuisce alla sicurezza del paziente fragile;
- favorisce un approccio più uniforme e standardizzato al rischio di delirium;
- riduce il carico assistenziale e sociale associato agli esiti del delirium nei pazienti anziani.

6. Supporto alla pianificazione sanitaria interna
I risultati possono essere utilizzati per:
- integrare lo score nei percorsi di accoglienza e valutazione dei pazienti anziani;
- formare il personale su un approccio sistematico e basato su evidenze nella prevenzione del delirium.

Potenziali rischi derivanti dalla sperimentazione allo studio:

Per la natura osservazionale dello studio, comprendente unicamente una fase retrospettiva, non sono previsti rischi addizionali rispetto a quelli già noti in relazione al normale trattamento di questa tipologia di pazienti.

Vi è un rischio aggiuntivo di accesso illegittimo ai dati di ricerca, che saranno protetti come sotto descritto in modo da minimizzare i rischi di trattamento.

3.1.2 Fasi del processo

3.1.2.1 Progettazione (definizione del protocollo)

Nella fase di progettazione è stata individuata una platea di soggetti rispondenti a determinati criteri (**criteri di eleggibilità**) e di **un numero di pazienti** che possa dare **significatività statistica allo studio**. Il numero di pazienti è stato individuato in un range di circa 700. Tuttavia, il numero di pazienti potrà subire variazioni in relazione all'andamento dello studio e alla natura dello stesso che comunque verranno notificate al Comitato Etico competente.
Sono stati individuati:
- Le ricerche già effettuate in materia
- Il set di dati da raccogliere

- Le correlazioni ipotizzate tra le diverse variabili
- La possibilità/opportunità di fornire feedback personalizzati agli utenti

La fase di progettazione si è conclusa con la predisposizione del protocollo dello studio che ha tenuto conto dei seguenti elementi:

- I criteri di eleggibilità
- I numeri di soggetti da coinvolgere: oltre il numero per la significatività statistica si è ipotizzato di aggiungere un margine per la gestione di eventi quali revoca del consenso, opposizione
- La valutazione della possibilità di informare gli interessati ed acquisire il relativo consenso. Si rimanda all'Autorizzazione Generale sulla ricerca scientifica[1] per un'esemplificazione dei suddetti casi:
    - Deceduti
    - Non contattabili
    - Non in grado di comprendere l'informativa stessa e/o esprimere un valido consenso

- I dati di partenza
- I dati da raccogliere per lo studio (dettaglio della CRF Case Report Form)
- La relativa codifica (IDC, etc.)
- La precisione dei dati da raccogliere
- Le procedure di data quality applicabili
- Il periodo di conservazione dei dati (20 anni) al termine dello studio
- L'elenco dei soggetti coinvolti
- L'individuazione degli strumenti di trattamento applicabili nelle diverse fasi
- Le procedure di eventuali scambi dati con altri soggetti
- Le norme che richiedono/su cui si basa la ricerca
- Gli standard applicabili
- I ruoli privacy
- Altri aspetti privacy (informativa, consenso, trasferimenti, rispetto dei principi)

La fase di progettazione ha tenuto conto dei requisiti degli artt. 5 e 25 del GDPR, per il cui dettaglio si rinvia al par. 194 - Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento.

3.1.2.2 <u>Fase di individuazione dei pazienti eleggibili</u>

Tale fase prevede, almeno come primo step, la consultazione delle seguenti basi dati:

---

[1] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9068972#5 Negli altri casi, quando non è possibile acquisire il consenso degli interessati, i titolari del trattamento devono documentare, nel progetto di ricerca, la sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, tra le quali in particolare:
1. i motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione. Rientrano in questa categoria le ricerche per le quali l'informativa sul trattamento dei dati da rendere agli interessati comporterebbe la rivelazione di notizie concernenti la conduzione dello studio la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi (possono rientrare in questa ipotesi, ad esempio, gli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso per il quale non esista un trattamento).
2. i motivi di impossibilità organizzativa riconducibili alla circostanza che la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile contattare per informarli, 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; ciò avuto riguardo, in particolare, 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 (ad esempio, nei casi in cui lo studio riguarda interessati con patologie ad elevata incidenza di mortalità o in fase terminale della malattia o in età avanzata e in gravi condizioni di salute).
Con riferimento a tali motivi di impossibilità organizzativa, le seguenti prescrizioni concernono anche il trattamento dei dati di coloro i quali, 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
- non contattabili.

- Cartella clinica cartacea

La consultazione viene condotta dal personale che partecipa alla Sperimentazione, producendo un'estrazione che contenga solamente:

- I dati previsti dalla CRF, possibilmente già con la precisione e la codifica definite nello studio.
- L'insieme dei dati di controllo previsti dalle procedure di data quality.

3.1.2.3 Pseudonimizzazione

Per quanto riguarda le tecniche di pseudonimizzazione utilizzate si rinvia al paragrafo 6.2.
In ogni caso, si considerano rispettati i criteri fissati dall'Allegato A5[2].

3.1.2.4 Fase di estrazione e copiatura nella CRF

I dati clinici saranno estratti manualmente, a cura di personale esperto e adeguatamente formato e inseriti nella CRF (foglio di calcolo).

In ogni caso non possono essere introdotte chiavi che anche in combinazione tra loro portano all'identificazione diretta del paziente, anche facendo uso di informazioni tenute logicamente ed organizzativamente separate. Nello specifico, la CRF dovrà avere come chiave quella individuata nello step di pseudonimizzazione.

3.1.2.5 Fase di data quality

Gli obiettivi di questa fase sono:

- L'accuratezza dei dati inseriti nella CRF
- La verifica che non vi è possibilità di single out di pazienti (K anonimato, L Diversity)

Tale fase può comportare eventuali aggregazioni e/o nuove generalizzazioni (da notificare eventualmente al comitato etico) o l'esclusione dallo studio di pazienti eleggibili ma "singoli" (per esempio un paziente molto anziano).

---

[2] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069637
Art. 4. Identificabilità dell´interessato. Agli effetti dell´applicazione delle presenti regole:
a) un interessato si ritiene identificabile quando, con l´impiego di mezzi ragionevoli, è possibile stabilire un´associazione significativamente probabile tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati che la identificano;
b) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie:
• risorse economiche;
• risorse di tempo;
• archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione;
• archivi, anche non nominativi, che forniscano ulteriori informazioni oltre quelle oggetto di comunicazione o diffusione;
• risorse hardware e software per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al software di controllo adottati;
• conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati;
Art. 5. Criteri per la valutazione del rischio di identificazione 1. Ai fini della comunicazione e diffusione di risultati statistici, la valutazione del rischio di identificazione tiene conto anche dei seguenti criteri:
a) si considerano dati aggregati le combinazioni di modalità alle quali è associata una frequenza non inferiore a una soglia prestabilita, ovvero un'intensità data dalla sintesi dei valori assunti da un numero di unità statistiche pari alla suddetta soglia. Il valore minimo attribuibile alla soglia è pari a tre;
b) nel valutare il valore della soglia si deve tenere conto del livello di riservatezza delle informazioni;
c) i risultati statistici relativi a sole variabili pubbliche non sono soggette alla regola della soglia;
d) la regola della soglia può non essere osservata qualora il risultato statistico non consenta ragionevolmente l'identificazione di unità statistiche, avuto riguardo al tipo di rilevazione e alla natura delle variabili associate;
e) i risultati statistici relativi a una stessa popolazione possono essere diffusi in modo che non siano possibili collegamenti tra loro o con altre fonti note di informazione, che rendano possibili eventuali identificazioni;
f) si presume adeguatamente tutelata la riservatezza nel caso in cui tutte le unità statistiche di una popolazione presentano la medesima modalità di una variabile.

A valle di questa fase, i dati verranno anonimizzati/de-identificati per le finalità di pubblicazione scientifica.

3.1.2.6 Fase di correlazione statistica

In questa fase si procede all'analisi statistica e si confermano (o meno) le ipotesi dello studio. Tipicamente sono utilizzate librerie di analisi statistica. Queste devono essere aggiornate e non comportare trasferimenti di dati a soggetti terzi.

Il Data manager/Bioinformatico del centro di sperimentazione si occuperà, su indicazione del Principal Investigator, di eseguire analisi di tipo descrittivo ed inferenziali per la verifica delle ipotesi. Qualora si rilevi in futuro la necessità di coinvolgere altri soggetti esterni, verranno rivalutati gli elementi del trattamento e i relativi ruoli privacy.

3.1.2.7 Fase di preparazione dei dati da pubblicare

Obiettivo di questa fase è la verifica che i dati da pubblicare siano realmente anonimi, con probabilità di re-identificazione estremamente bassa, verificando che non vi è possibilità di single out di pazienti (K anonimato, L Diversity).

3.1.2.8 Fase di estrazione dei dati per altri progetti di ricerca

Obiettivo di questa fase eventuale è l'estrazione dei dati per poter svolgere ulteriori studi. In base al Parere del Garante all'AOU di Verona 30 giugno 2022 [9791886], occorre ricontattare i pazienti per acquisirne uno specifico consenso, tranne nei casi in cui si possa procedere altrimenti (ex art. 100bis c4). Se sussistono pazienti che non possano prestare il proprio consenso e non escludibili dal nuovo studio occorre procedere ai sensi dell'art. 110 Codice Privacy.
In questo caso vale quanto sopra esposto relativamente alle fasi progettazione, eleggibilità, pseudonimizzazione. Vanno adottate misure per garantire la riservatezza in fase di trasmissione dei dati agli investigatori del nuovo studio.

3.1.2.9 Fase di anonimizzazione/cancellazione dei dati

Obiettivo di questa fase è assicurare la completa non collegabilità dei dati ai singoli pazienti.
Stante la natura e la finalità dello studio in oggetto, si ritiene opportuno conservare la tabella di correlazione per un periodo di 5 anni successivi al termine dello studio.
In seguito, si procederà con la cancellazione sicura (fisica) di tutti i supporti (principali e copie di backup) su cui sono conservati i dati anagrafici di correlazione.
Inoltre, saranno impiegate le tecniche di de-identificazione indicate nel WP 216 - 5/2014 per i dati personali contenuti nella CRF. Inizialmente, si procederà ad aggregare i dati sostituendo quelli puntuali con la media su insiemi di pazienti numericamente elevati (oltre i 30) e verranno eliminate tutte le date sostituendole con il solo anno solare.
Verranno inoltre applicati controlli di K-anonimato e L-diversity con valore K=30 e L=15 su tutti dati particolari, eliminando eventuali variabili che non soddisfino il requisito.
Si procederà in accordo alla ISO/IEC 27559:2022 a verificare periodicamente l'efficacia della procedura di de-identificazione e la robustezza degli algoritmi di crittografia anche tenendo conto delle Linee Guida sulle funzioni crittografiche – Conservazione delle password pubblicate dal Garante e ACN.

3.1.3 Ruoli e responsabilità collegate al trattamento.

I soggetti che possono intervenire oltre il Titolare del trattamento sono:

- Fornitore Dedalus Italia S.p.A., in qualità di Responsabile del trattamento per le attività di assistenza/manutenzione IT

Vi sono altri soggetti (Comitato Etico, AIFA) che possono intervenire nel processo per le verifiche di competenza.

In ogni caso il personale che accede ad archivi contenenti dati personali anche solo indirettamente identificativi è stato autorizzato se subordinato/parasubordinato oppure nominato Responsabile ex art. 28 GDPR negli altri casi.

3.1.3.1.1 Persone fisiche che intervengono nel trattamento

Nel trattamento intervengono:

- **L'investigatore/sperimentatore principale**: **definisce il protocollo**: assume il ruolo di designato/delegato, cioè di autorizzato con ruolo di impostazione e coordinamento
- **Investigatori/Sperimentatori**: coordinati dall'investigatore principale raccolgono i dati
- **Data manager**: figura non sanitaria che raccoglie e sistematizza i dati. Spesso operano tramite contratti di lavoro parasubordinati con l'Università o con l'Azienda sanitaria. Può essere visto come autorizzato, eventualmente con compiti di Amministratore di sistema in quanto abilita i ricercatori all'applicativo di CRF. Dovrebbe avere conoscenze di pseudonimizzazione e di statistica. Supporta la definizione della CRF e applica ai dati sanitari le trasformazioni di anonimizzazione.
- **Statistico**: ha la responsabilità di condurre i test statistici sui dati: può essere considerato un designato. Se i dati sono sufficientemente de identificati (dati anonimi) potrebbe non avere ruoli privacy

3.1.3.2 Correlazione tra i soggetti e le fasi

Fase	Soggetti giuridici	Persone fisiche
3.1.2.1 Progettazione (definizione del protocollo)	Ente Sperimentatore principale (Titolare)	Investigatore Principale
3.1.2.2 Fase di individuazione dei pazienti eleggibili	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale/Investigatore
3.1.2.3 Pseudonimizzazione	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale/Data Manager
3.1.2.4 Fase di copiatura nella CRF	Ente che ha raccolto/ricevuto i dati (Titolare),	Investigatore Principale/Data Manager
3.1.2.5 Fase di data quality	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale/Data Manager
3.1.2.6 Fase di correlazione statistica	Ente che ha raccolto/ricevuto i dati (Titolare)	Statistico
3.1.2.7 Fase di preparazione dei dati da pubblicare	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale/Data Manager
3.1.2.8 Fase di estrazione dei dati per altri progetti di ricerca	Ente che ha raccolto/ricevuto i	Investigatore Principale/Data Manager

	dati (Titolare)	
3.1.2.9 Fase di anominimizzazione/cancellazione dei dati	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale/Data Manager

3.2 Dati, processi e beni di supporto

3.2.1 Dati trattati

I dati personali relativi ai pazienti arruolati sono definiti nel protocollo di studio presentato al Comitato Etico.

Dati personali del paziente:

- Dati anagrafici: nome, cognome, età, sesso;
- Dati relativi alla salute: diagnosi nota di deterioramento cognitivo; deficit uditivo documentato; uso cronico di farmaci psicotropi (quali antidepressivi, antipsicotici, antiepilettici, oppioidi, farmaci anti-Parkinson, farmaci anti-demenza); valutazione delle comorbidità tramite Charlson Comorbidity Index (CCI); durata della degenza; esito del ricovero.

Per l'adozione delle necessarie misure di sicurezza si trattano i seguenti dati degli operatori (Investigatori, Data Manager).

- Dati anagrafici
- Credenziali di accesso
- Fattore di autenticazione (password, numero cellulare, ID token)
- Mail
- Log delle operazioni effettuate (indirizzo IP della postazione/account, data e ora di esecuzione, tipologia di operazione compiuta)

I log di windows registrano le operazioni di accesso al sistema da parte degli utenti.

3.2.2 Fonti dei dati

I dati dei pazienti utilizzati per le finalità dello studio sono acquisiti da cartelle cliniche e documentazione sanitaria

3.2.3 Descrizione del flusso dei dati

3.2.3.1 Flusso dei dati

Si veda il capitolo 3 - Fase 1: Descrizione del trattamento.

3.2.3.2 Tipo di operazioni

La tipologia delle operazioni effettuate sono:

Operazioni standard: Raccolta, Registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.

Operazioni particolari: nessuna.

Comunicazione mediante trasmissione: I dati personali non sono comunicati a soggetti terzi., salva l'ipotesi di estrazione dei dati per altri progetti di ricerca, indicata al paragrafo 3.1.2.8.

Diffusione: I dati potranno essere diffusi in forma aggregata per pubblicazioni scientifiche.

Profilazione: Nell'ambito di tali trattamenti i dati personali non sono oggetto di processi decisionali automatizzati né di profilazione (ovvero una qualsiasi forma di trattamento automatizzato per valutare determinati aspetti personali, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica) su cui si basi una decisione o che produca un effetto giuridico sull'interessato o che incide significativamente sulla sua persona.

3.2.4 Beni di supporto

I beni di supporto possono essere raggruppati in:

- Fonti dei dati:
    - Cartelle cliniche e documentazione sanitaria
- Sistema per la gestione della CRF (e-CRF)
    - Fogli di calcolo Excel (Microsoft Office 2309 build 16827.20166)

Infrastruttura:

- Computer dedicato, fisicamente localizzato presso S.C. Medicina Interna – Ospedale Santa Croce di Moncalieri
- Share di rete su server aziendale ubicati presso il CED
- Firewall
- Rete: Intranet aziendali, connessioni da rete pubblica

I documenti cartacei vengono archiviati presso il reparto Medicina Interna – Ospedale Santa Croce di Moncalieri sotto la responsabilità del Principal Investigator in armadio provvisto di chiave.

4. Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento

4.1 Proporzionalità e necessità

Lo scopo di miglioramento del processo di cura/prevenzione e più in generale della salute della collettività si viene a contrappore al diritto alla riservatezza dei singoli. Il miglioramento è tanto più urgente quanto le patologie hanno effetti socioeconomici importanti. D'altra parte, gli impatti sui pazienti sono tanto maggiori quanto le patologie destano allarme sociale e potenziale discriminazione.

I dati personali sono indispensabili per la qualità della ricerca. Le fasi di verifica dei risultati sono un requisito fondamentale di un processo di qualità. Queste, quindi, richiedono una collegabilità del dato alle informazioni cliniche primarie e di conseguenza all'identità del paziente. La strategia principale per rendere il trattamento il meno impattante possibile sulla riservatezza è la minimizzazione della collegabilità tramite tecniche di minimizzazione e pseudonimizzazione dei dati.

4.1.1 Finalità esplicite e legittime

Le finalità del trattamento sono:

1) Di ricerca scientifica come illustrato nel protocollo
2) Didattiche: in particolare la presentazione a convegni

Esse vengono esplicitate nell'informativa (cfr. Allegato 2).

4.1.2 Fondamenti legali del trattamento

La base giuridica del trattamento si fonda su:

- Limitatamente al trattamento dei dati personali dei pazienti non contattabili per la fase retrospettiva, art. 110 d.lgs. 196/2003 (valutazione d'impatto ai sensi dell'art. 35 del GDPR e applicazione di misure a garanzia ai sensi dell'art. 106, comma 2, lettera d) del d.lgs 196/2003.
- Nel caso di specie per alcuni interessati non è stato possibile acquisire il consenso in quanto risulta impossibile o uno sforzo sproporzionato contattarli.

4.1.3 I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario al conseguimento delle finalità del trattamento ("Minimizzazione dei dati")

Ogni dato raccolto è direttamente e specificatamente funzionale alle necessità per le quali è stato raccolto ed è pertanto pertinente rispetto alle finalità sopra esplicitate. Nell'Allegato 1 a fianco di ogni campo sono illustrate le ragioni che impongono il trattamento.

4.1.4 Accuratezza ed aggiornamento dei dati

Gli Sperimentatori verificano la correttezza dei dati raccolti sulla scheda raccolta dati confrontandoli con quelli presenti sulla cartella clinica del partecipante. I dati sono raccolti e trattati da un numero ristretto di persone: Principal Investigator e personale del gruppo di ricerca autorizzato.
Si assume che la documentazione clinica di origine (cartella clinica) sia accurata (documento di fede privilegiata).
Le procedure di data quality previste sono tese a verificare queste proprietà del dato.

I dati verranno trattati mediante processo di pseudonimizzazione, ovvero ad ogni soggetto partecipante allo studio verrà assegnato un codice che verrà utilizzato nello studio, come descritto nel paragrafo 6.2. La chiave per risalire all'oggetto sarà conosciuta solo dal Principal Investigator e dai ricercatori del gruppo di ricerca autorizzati dal PI.
I dati raccolti saranno oggetto di un'attività di anonimizzazione, sulla base del WP 216 5/2014 per la pubblicazione e alla fine dello studio.

4.1.5 Durata della conservazione dei dati

I dati in forma direttamente identificabile sono conservati a norma di legge nella documentazione clinica (ambito escluso dalla presente DPIA).

La CRF e la tabella di correlazione contenenti i dati anagrafici e direttamente identificativi del paziente saranno conservati in modalità segregata per 2 mesi dopo il termine dello studio.
Tale periodo di conservazione si rende necessario al fine di costruire analisi e studi futuri, volti a migliorare le conoscenze demografiche, cliniche, diagnostiche e terapeutiche e la pratica clinica.

I risultati dello studio (dati anonimi) verranno conservati a tempo indeterminato.

I dati di autorizzazione, identificazione ed accesso ai sistemi sono conservati per 1 anno.

È fatta salva, come detto in precedenza, la conservazione dei dati personali, anche particolari, per un periodo superiore, nei limiti del termine di prescrizione dei diritti, in relazione ad esigenze connesse all'esercizio del diritto di difesa in caso di controversie.

4.2 Controlli per proteggere i diritti degli interessati

4.2.1 Come sono informati gli interessati circa il trattamento

Ai pazienti contattabili viene fornita l'informativa privacy al primo accesso utile alla Struttura del Titolare, comprensiva di acquisizione del consenso.

Per i pazienti non contattabili, la relativa informativa verrà pubblicata sul sito web istituzionale, con richiamo nella sezione News e in un box dedicato, al fine di fornire adeguata pubblicità del trattamento per tutti i casi di impossibilità di contatto con i singoli interessati (o di altre ragioni per la non acquisizione del consenso), in ossequio alle regole deontologiche sulla ricerca scientifica Allegato A5 Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018.
Si rinvia all'Allegato 2 per la consultazione delle informative e all'allegato 3 per la consultazione dell'Avviso sullo Studio.

4.2.2 Esercizio dei diritti da parte degli interessati

Per esercitare i diritti previsti dagli artt. da 15 a 22 del GDPR, l'interessato può rivolgersi al titolare del trattamento, anche per il tramite del DPO. I diritti possono essere esercitati con le modalità indicate nell'informativa.
Inoltre, come precisato nell'informativa, l'interessato può sempre esercitare, qualora ritenga che il trattamento dei Suoi dati personali avvenga in violazione di quanto previsto dal GDPR, il diritto di proporre reclamo all'Autorità di controllo, seguendo le indicazioni pubblicate sul sito della stessa (https://www.garanteprivacy.it/modulistica-e-servizi-online/reclamo) o di ricorrere avanti la competente autorità giudiziaria (artt. 77 e 79 del GDPR).

4.2.2.1 Diritto di accesso

Con riferimento al diritto di accesso, l'interessato può ottenere la conferma che sia o meno in corso un trattamento di dati che lo riguardano e in tal caso ottenere l'accesso agli stessi e alle informazioni riportate in dettaglio all'art. 15 del GDPR (es. finalità, destinatari, periodo di conservazione).

4.2.2.2 Diritto di rettifica

L'interessato, inoltre, ha sempre il diritto di ottenere – senza ingiustificato ritardo e comunque entro un mese - la rettifica dei dati personali inesatti che lo riguardano ovvero l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

4.2.2.3 Diritto di cancellazione

Per il trattamento in oggetto che si fonda sul consenso, l'interessato potrà richiedere la cancellazione dei dati personali nell'ambito del presente studio, ai sensi dell'art. 17 del GDPR.

Per quanto concerne, invece, il trattamento dei personali fondato sull'art. 110 del Codice Privacy, il diritto alla cancellazione dei dati potrà essere esercitato anche per il tramite dei soggetti legittimati ai sensi dell'art. 2-terdecies del Codice Privacy.

4.2.2.4 Diritti di limitazione

L'interessato ha il diritto di chiedere la limitazione del trattamento quando:

a. contesta l'esattezza dei dati personali, chiedendo quindi la rettifica, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b. ritiene che il trattamento sia illecito e chiede che ne sia limitato l'utilizzo;
c. i dati personali sono necessari per l'accertamento, l'esercizio o la difesa di un diritto dell'interessato in sede giudiziaria;
d. si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

4.2.2.5 Diritto di opposizione

L'interessato ha il diritto di opporsi al trattamento per motivi connessi alla sua situazione particolare. Il Titolare dovrà astenersi dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. (art. 21 del GDPR).

4.2.3 Obbligazioni dei responsabili del trattamento

Dedalus Italia S.p.A. è stato individuato quale responsabile del trattamento *ex* art. 28 del GDPR con apposito atto di nomina.

4.3 Trasferimenti al di fuori dello SEE

Non vengono effettuati trasferimenti al di fuori dello Spazio Economico Europeo.

4.4 Rispetto dei principi di Privacy by Design

4.4.1 Rispetto delle strategie

1. Minimizzare: sono trattati soltanto i dati necessari per raggiungere le finalità
2. Aggregare: sono applicate misure di pseudonimizzazione che prevedono tale strategia
3. Nascondere: il trattamento dei dati personali è limitato soltanto a soggetti autorizzati ed i dati vengono conservati in forma cifrata
4. Informare: all'interessato sono fornite tutte le informazioni pertinenti al trattamento in oggetto (informative ex art. 13 GDPR)
5. Controllare: all'interessato è garantito l'esercizio dei diritti previsti dalla normativa (artt. 15-22 GDPR). Si rinvia alla procedura di gestione dei diritti degli interessati.
6. Dimostrare: si rinvia alle policy del Titolare del trattamento

5. Fase 3: Calcolo del livello del rischio

Il livello del rischio viene calcolato moltiplicando il valore dell'Impatto (conseguenze negative per gli Interessati di una determinata minaccia) per la Probabilità che una determinata minaccia si possa verificare.
Pertanto, il livello del rischio è pari:

LIVELLO DEL RISCHIO = IMPATTO X PROBABILITÀ OCCORRENZA DELLA MINACCIA

5.1 Calcolo dell'impatto

Si considerano i seguenti livelli di Impatto:

Tabella 1

LIVELLO DI IMPATTO	VALORE	DESCRIZIONE
BASSO	1	Gli individui possono andare incontro a **disagi minori**, che supereranno **senza alcun problema** (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
MEDIO	2	Gli individui possono andare incontro a **significativi disagi**, che saranno in grado di superare nonostante **alcune difficoltà** (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
ALTO	3	Gli individui possono andare incontro a **conseguenze significative**, che dovrebbero essere in grado di superare anche se con **gravi difficoltà** (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
MOLTO ALTO	4	Gli individui possono subire **conseguenze significative**, o addirittura irreversibili, **non superabili** (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Il livello d'Impatto deve essere valutato in relazione alle seguenti variabili:

- perdita di riservatezza dei dati;
- perdita d'integrità dei dati;
- perdita di disponibilità dei dati.

Tabella 2

N.	DOMANDA	VALUTAZIONE
I.1.	Si prega di riflettere sull'impatto che una divulgazione non autorizzata (perdita di riservatezza) dei dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/*rating* di conseguenza.	O **BASSO (1)** O **MEDIO (2)** X **ALTO (3)** O **MOLTO ALTO (4)**
I.2.	Si prega di riflettere sull'impatto che un'alterazione non autorizzata (perdita di integrità) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività – potrebbe avere sull'individuo ed esprimere una valutazione/*rating* di conseguenza.	X **BASSO (1)** O **MEDIO (2)** O **ALTO (3)** O **MOLTO ALTO (4)**

I.3.	Si prega di riflettere sull'impatto che una distruzione o perdita non autorizzata (perdita di disponibilità) di dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/ *rating* di conseguenza.	**X BASSO (1)** O **MEDIO (2)** O **ALTO (3)** O **MOLTO ALTO (4)**

Il più alto dei tre livelli (perdita di riservatezza, integrità e disponibilità) deve essere considerato come il risultato finale della valutazione dell'Impatto.

Tabella 3

LIVELLO FINALE DELL'IMPATTO	**ALTO**

5.2 Calcolo della probabilità di accadimento della minaccia

Si deve ora valutare la Probabilità di accadimento delle minacce correlate al trattamento di dati personali nell'ambito del progetto in base al contesto complessivo del trattamento (esterno o interno). Per semplificare questo processo, sono state definite una serie di domande di valutazione (**Tabella 5**) che mirano a sensibilizzare sull'ambiente di elaborazione dei dati (che è direttamente rilevante per le minacce). In tale prospettiva, le domande sono suddivise in quattro diverse aree di valutazione:

1. risorse tecniche e di rete;
2. processi / procedure relativi all'operazione di trattamento dei dati;
3. parti / persone coinvolte nel trattamento dei dati personali;
4. settore di operatività e scala di trattamento.
5. per ciascuna delle predette aree deve essere valutato il livello di probabilità di occorrenza della minaccia in base alla seguente scala:

Tabella 4

Basso	è improbabile che la minaccia si materializzi	Punteggio 1
Medio	c'è una ragionevole possibilità che la minaccia si materializzi	Punteggio 2
Alto	la minaccia potrebbe materializzarsi	Punteggio 3

Tabella 5

RISORSE DI RETE E TECNICHE		
QUESITO	**ESEMPIO**	**RISPOSTA**
Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?	Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte di aggressori esterni online (ad esempio *Denial of Service*, *SQL injection*, attacchi *Man-in-the-Middle*), soprattutto quando il servizio è disponibile (e, quindi, rintracciabile / noto) a tutti gli utenti di Internet.	**SI**
È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?	Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in spazi pubblici). Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione / amministrazione remota del sistema IT.	**NO**

Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunamente configurati, tali connessioni possono consentire l'accesso (ai dati personali) a più persone all'interno dell'organizzazione (che in linea di principio non sono autorizzate a tale accesso).	**NO**
Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente all'IT, apparecchiature e componenti di rete, o non riuscendo a fornire protezione della sala computer in caso di disastro fisico).	**NO**
Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?	Componenti hardware e software mal progettate, implementate e / o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono dopo l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione (ai rischi) e raggiungere determinati livelli di resilienza.	**NO**
PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI		
QUESITO	**ESEMPIO**	**RISPOSTA**
I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema	**NO**
L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	Quando un uso accettabile delle risorse non è chiaramente obbligatorio, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio, intenzionale del sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali.	**NO**
I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema *bug* o virus aggiuntivi.	**NO**
I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. rete wifi aperte)	**NO**
Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/ procedure e risorse, con conseguente abuso di dati personali	**SI**
PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI		
QUESITO	**ESEMPIO**	**RISPOSTA**

Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	Quando l'accesso (e l'ulteriore trattamento) dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali.	**NO**
Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	Quando l'elaborazione viene eseguita da contraenti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. È importante che l'organizzazione selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo.	**NO**
Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo	**NO**
Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza.	**NO**
Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzo non autorizzati.	**NO**
SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO		
QUESITO	**ESEMPIO**	**RISPOSTA**
Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore dell'organizzazione del Titolare del trattamento, questa è un'indicazione che l'organizzazione probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile	**SI**
La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	Se l'organizzazione è già stata attaccata o ci sono indicazioni che questo potrebbe essere stato il caso, è necessario prendere ulteriori misure per prevenire eventi simili in futuro.	**NO**
Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	*Bug* di sicurezza / vulnerabilità possono essere sfruttati per eseguire attacchi (*cyber* o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra.	**NO**
Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	Il tipo e il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati).	**SI**
Esistono *best practice* di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni (e ai rischi) del particolare settore. La mancanza di conformità con le migliori pratiche pertinenti potrebbe essere un indicatore di scarsa gestione della sicurezza.	**NO**

CRITERI PER CALCOLARE IL LIVELLO DI PROBABILITA' (Tabella 6)		
DOMANDE	**RISPOSTE**	**CRITERIO PER CALCOLO DEL RISCHIO PER SEZIONE**
RISORSE DI RETE E TECNICHE		
Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?	**SI'**	La valutazione complessiva di questa sezione sarà: BASSO: se si hanno fino a 2 SI MEDIO: se si hanno 3 SI ALTO: se si hanno 4 o 5 SI
È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?	**NO**	
Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	**NO**	
Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	**NO**	
Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?	**NO**	
PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI		
I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	**NO**	La valutazione complessiva di questa sezione sarà: MEDIO: se si risponde SI alle domande n.3 e n.4, in quanto il livello di rischio per questa sezione non può essere considerato 'basso' quando i comportamenti dei dipendenti possono essere causa di perdita di integrità, riservatezza e disponibilità dei dati
L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	**NO**	
I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	**NO**	
I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	**NO**	
Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	**NO**	

PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI		
Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	**NO**	La valutazione complessiva di questa sezione sarà: BASSO: se si risponde NO alla domanda n.2, in quanto significa che i dati vengono trattati all'interno dei sistemi del Titolare garantendone così allo stesso il pieno controllo MEDIO: se si risponde SI alla domanda n.2, in quanto il coinvolgimento di un terzo fa sì che ci sia meno controllo sul trattamento dei dati stessi
Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	**NO**	
Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	**NO**	
Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	**NO**	
Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	**NO**	
SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO		
Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	SI	La valutazione complessiva di questa sezione sarà: BASSO: se si risponde NO alla domanda n.4, infatti se il sistema IT utilizzato non elabora quantità elevate di dati, il rischio è da considerarsi contenuto MEDIO: se si risponde SI alla domanda n.4, infatti un volume elevato di dati personali conservati ed elaborati in un sistema IT aumenta il rischio dell'impatto di eventuali incidenti di sicurezza ALTO: se dovessero variare i parametri e dovessero esserci 3 o più sì
La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	NO	
Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO	
Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	SI	
Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO	

Tabella 6

AREA DI VALUTAZIONE	PROBABILITA'	
	LIVELLO	PUNTEGGIO
RETE E RISORSE TECNICHE	Basso	1
	Medio	2
	Alto	3
PROCESSI / PROCEDURE RELATIVI AL TRATTAMENTO DEI DATI PERSONALI	Basso	1
	Medio	2
	Alto	3
PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	Basso	1
	Medio	2
	Alto	3
SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	Basso	1
	Medio	2
	Alto	3

I punteggi attribuiti alle 4 aree nella **Tabella 6** devono essere sommati per calcolare il valore finale di probabilità di occorrenza della minaccia fissato in base alla **Tabella 7** che segue.

Tabella 7

Somma globale della probabilità di occorrenza di una minaccia	LIVELLO DI PROBABILITÀ DELLE MINACCE
4 - 5	Basso
6 - 8	Medio
9 -12	Alto

Nella valutazione finale del livello di Probabilità si è tenuto conto anche delle seguenti considerazioni in relazione alla:

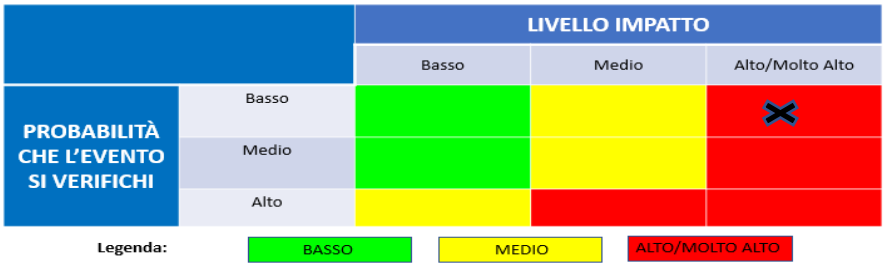
In base alle valutazioni effettuate il livello finale della probabilità di occorrenza delle minacce viene stimato:

Tabella 8

LIVELLO FINALE DELLA PROBABILITÀ DELLE MINACCE	**BASSO**

5.3 Calcolo del livello di rischio

Il livello del rischio sarà dato dalla moltiplicazione del risultato del livello d'Impatto riportato nella **Tabella 3** del paragrafo 5.1 per il risultato del livello di probabilità riportato nella **Tabella 8** del paragrafo 5.2.



LIVELLO DEL RISCHIO	**ALTO**

5.4 Individuazione delle misure che mitigano il rischio

Determinato il livello del rischio, e individuate le minacce e le fonti che potrebbero concretizzarlo, vengono individuate ora le misure di sicurezza che contribuiscono alla mitigazione del rischio stesso.

Perdita di riservatezza

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Le principali minacce relative alla perdita di riservatezza riguardano comportamenti umani quali, ad esempio, condivisione dei dati personali con soggetti non autorizzati, errori nelle configurazioni di sicurezza dei sistemi informatici che permettono accessi illegittimi, attacchi informatici esterni, violazione di account.

Quali sono le fonti di rischio?

Le fonti di rischio sono quindi costituite principalmente da operatori interni mal istruiti o insoddisfatti, attacchi esterni tramite phishing, social engineering o sfruttamento di vulnerabilità.

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità di accadimento delle minacce?

La probabilità di accadimento delle minacce è mitigata da diverse misure che verranno descritte nel dettaglio nel paragrafo 6. In particolare, le misure che maggiormente contribuisco a garantire una maggior tutela della riservatezza sono la pseudonimizzazione e la prevenzione del malware.

- I dati contenuti nella Base Dati sono infatti pseudonimizzati e non permettono quindi di risalire direttamente all'identità degli Interessati. I dati contenenti la corrispondenza tra i dati anagrafici dei pazienti e il codice identificativo sono infatti salvati separatamente, come indicato nella sezione dedicata.
- I dati della CRF ed i dati identificativi sono soggetti a protezione crittografica (Excel protetto da password di accesso)
- Gli accessi fisici sono controllati e le postazioni gestite.
- IL PC sarà tenuto acceso solo durante l'utilizzo effettivo
- Il PC non sarà accessibile via VPN e comunque da remoto: verranno disabilitati/disinstallati i relativi servizi
- Viene erogata regolare formazione agli autorizzati al trattamento.
- Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, crittografia, gestione del personale, vulnerabilità.

Perdita d'integrità

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Le principali minacce relative alla perdita di integrità riguardano ridotti controlli di qualità sulle procedure

di data entry. L'errore più probabile potrebbe essere un errore nel mappaggio tra il dato originale e la codifica standard di riferimento. I rischi potrebbero, inoltre, concretizzarsi a seguito di attacchi informatici ed errori umani.

Quali sono le fonti di rischio?

Le fonti di rischio principali riguardano: un operatore interno mal istruito o insoddisfatto, attaccante esterno tramite phishing, social Engineering o sfruttamento di vulnerabilità.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Le misure, meglio descritte nel paragrafo 6, adottate per mitigare i rischi di perdita d'integrità sono le seguenti:
Prima di tutto vengono eseguiti diversi controlli di qualità sui dati (descritti alla sezione 3.1.2.5) che ne garantiscono l'integrità: controlli di qualità a campione, revisione programmatica delle statistiche descrittive.
Gli accessi ai dati personali sono permessi solo a seguito di autenticazione attribuendo i permessi sulla base dei ruoli ricoperti.
Gli accessi fisici sono controllati e le postazioni gestite.
Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, crittografia, vulnerabilità.

Perdita di disponibilità

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

La principale minaccia relativa alla perdita di disponibilità riguarda la distruzione accidentale della Base Dati o fisica del server.

Quali sono le fonti di rischio?

Le fonti di rischio per una perdita di disponibilità sono: attività volontaria di un operatore interno con accesso alla Base Dati; attaccante esterno tramite phishing, social Engineering o sfruttamento di vulnerabilità. Errore umano interno per disattenzione/incompetenza. Perdita della password.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Le misure adottate per mitigare la perdita di disponibilità dei dati, meglio descritte nel paragrafo 6, riguardano principalmente la presenza di un backup su una cartella di storage dedicata, gestita a cura dei sistemi informativi del Titolare.
Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici e degli accessi fisici, archiviazione, partizionamento, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, vulnerabilità, lotta contro il malware, gestione postazioni, gestione dei rischi, gestione del personale, sicurezza dei canali informatici, sicurezza dell'hardware e vigilanza sulla protezione dei dati.

6. Fase 4: Misure di mitigazione adottate

6.1 Crittografia - Cifratura

Vengono implementate le seguenti tecniche di cifratura dei dati personali:

- I dati trasferiti durante le attività di backup sono trasmessi su canali sicuri.
- I dati della CRF sono oggetto di cifratura tramite l'utilizzo di una password per il database Excel.
- Il file relativo alle corrispondenze e il database Excel saranno protetti tramite password differenti con criteri di robustezza quali:
    - Lunghezza minima 14 caratteri
    - Lettere maiuscole e minuscole
    - Cifre di base 10 (da 0 a 9)
    - Caratteri non alfanumerici

La share di rete è crittografata con Bitlocker. Le chiavi crittografiche vengono conservate in share di rete dedicata accessibile soltanto agli Amministratori di Sistema autorizzati.

6.2 Pseudonimizzazione

Vengono implementate tecniche di pseudonimizzazione, al fine di ottenere la separazione tra i dati identificativi del paziente e i dati della CRF in accordo con gli standard di cui al par. 1.4, in particolare l'Opinione 05/2014 del WP29 e la recente NIST SP 800-188.
I dati direttamente identificativi non sono presenti nella CRF essendo sostituiti da una chiave di pseudonimizzazione scelta randomicamente e successivamente sottoposta ad un controllo di univocità.
Non viene, inoltre, riportata la data di nascita del paziente essendo stata sostituita con l'età alla prima diagnosi. Sono invece presenti date puntuali collegate ai diversi episodi, in quanto ritenute fondamentali per le analisi oggetto dello studio. Tali date potrebbero costituire insieme ad altri identificativi indiretti una potenziale individuazione del paziente solo tramite accesso alla documentazione clinica originaria, salvo una puntuale conoscenza personale del paziente da parte dell'eventuale attaccante che potrebbe comportare l'inferenza di ulteriori informazioni sanitarie.
Si ritiene, tuttavia, questo rischio contenuto.

I dati verranno organizzati utilizzando Fogli di Calcolo di Microsoft Excel, suddivise come di seguito precisato:

1. Tabella "Record paziente" [contiene dati potenzialmente identificativi (solo per la fase iniziale di estrazione)]:

- cognome e nome;
- età;
- sesso;
- data di ricovero e dimissione

2. Tabella "Informazioni cliniche e diagnostiche" (contiene esclusivamente dati sanitari utili allo studio):

- punteggi giornalieri del test 4AT;
- variabili necessarie al calcolo dello Zucchelli Score:

    - età >75 anni;
    - anamnesi di demenza;
    - deficit uditivo;
    - utilizzo di terapia psicotropa in cronico;
- Charlson Comorbidity Index;
- esiti clinici (durata degenza, esito alla dimissione);

Le tabelle saranno collegate per mezzo di un identificativo paziente random univoco (Codice alfanumerico costituito da 8 caratteri es: 6VHNOT#7)
La corrispondenza tra nominativo del paziente e il Codice univoco sarà registrata su file Excel separato.

Il responsabile dei dati e della loro pseudonimizzazione è lo sperimentatore principale.

6.3 Controllo degli accessi logici

La sicurezza degli accessi prevede l'identificazione degli utenti tramite le credenziali nominative di dominio e la concessione del pertinente profilo di autorizzazione, determinato sulla base dei privilegi concessi al singolo utente.

Per gli accessi degli "amministratori di sistema" vengono applicate le disposizioni di cui al provvedimento del garante del 2008 e della circolare AGID per le misure di sicurezza della 18/04/2017.

6.4 Tracciabilità

Non vengono tracciati

6.5 Minimizzazione dei dati

La raccolta dei dati si limita a quelli strettamente necessari a perseguire le finalità del trattamento.

- Le fasi di progettazione dello studio ha implicato il rispetto del principio di minimizzazione
- Lo sperimentatore garantisce che i dati previsti nella CRF sono i soli indispensabili alla conduzione dello studio
- L'esperto statistico garantisce che il numero di interessati è il minimo per dare rilievo allo studio

6.6 Lotta contro il malware

Il computer sarà su dominio aziendale e disporrà delle ultime patch di sicurezza nonché antivirus aziendale aggiornato secondo le policy aziendali.

È presente un Next generation firewall (Fortigate) con specifiche funzionalità antimalware.

- È pianificato specifico audit sulla configurazione dell'apparato.
- Sulle postazioni dedicate al trattamento sono state inibite la navigazione in internet e la ricezione della posta elettronica.
- Ciascuna postazione di lavoro è dotata di software antivirus, costantemente aggiornato in modo automatico.

- Sono state impartite specifiche disposizioni per verificare puntualmente l'aggiornamento sui sistemi interessati.

In estrema sintesi sono applicati a livello infrastrutturale:
- Strumenti anti "programmi pericolosi" (e.g. antivirus aggiornato periodicamente)
- Strumenti antintrusione (e.g. impiego di "firewall", segmentazione della rete, ecc.)

6.7 Vulnerabilità

Viene assicurata la protezione contro le vulnerabilità attraverso l'attuazione di una manutenzione ordinaria dei sistemi aziendali per l'applicazione di patch di sicurezza.

Inoltre, la protezione contro le vulnerabilità è garantita attraverso le seguenti attività:
- formazione del personale incaricato al trattamento dei dati
- aggiornamento del sistema almeno annuale
- utilizzo di software e sistemi operativi supportati dal produttore
- sincronizzazione NTP
- piani di risposta agli incidenti

6.8 Backup

Le politiche di backup prevedono che verrà eseguito il backup dei fogli e del database Excel su una cartella di storage dedicata messa a disposizione dai sistemi informativi con cadenza giornaliera o comunque ogni qualvolta vengano aggiunti/aggiornati i dataset.

A livello infrastrutturale vengono implementate le seguenti policy:
- I dati salvati hanno validità (retention) di 2 settimane.
- È previsto inoltre il backup automatico ogni 6 ore dei file presenti nella cartella condivisa.
- I backup sono monitorati e in caso di malfunzionamenti vengono attivate le opportune procedure per l'intervento correttivo.

6.9 Archiviazione

I dati cartacei sono conservati presso la sede dello studio dello sperimentatore Principale.

I dati trattati tramite fogli di calcolo Excel e sono conservati su un computer dedicato presso S.C. Medicina Interna dell'Ospedale Santa Croce di Moncalieri. Le password per l'accesso ai fogli di calcolo e al database crittografato verranno custodite presso l'ufficio del Principal investigator in apposito luogo sicuro.

Con cadenza quotidiana i file verranno caricati su una share di rete messo a disposizione dai servizi informativi dell'Azienda. Alla share di rete potranno accedere solo il data manager, il responsabile scientifico del progetto ed eventualmente altri membri della stessa S.C. Medicina Interna.

6.10 Sicurezza dei documenti cartacei

Non sono previsti documenti cartacei.

6.11 Sicurezza dell'hardware

Il computer sarà su dominio aziendale e disporrà delle ultime patch di sicurezza.

Come ulteriore misura di protezione l'hard disk del computer verrà cifrato utilizzando Bitlocker.

Sono applicate le opportune configurazioni di sicurezza relative all'hardware.

6.12 Gestione postazioni

La gestione delle postazioni comprende la postazione di lavoro dedicata, fisicamente localizzata presso l'ambulatorio del direttore della S.C. Medicina Interna – Ospedale Santa Croce di Moncalieri che viene chiuso a chiave.
Al computer dedicato per le attività avranno accesso solo il Data Manager e il responsabile scientifico del progetto.

Il computer resterà acceso solo durante il suo utilizzo.

Il Titolare ha predisposto un Regolamento per l'utilizzo dei dispositivi informatici, il quale prevede l'applicazione di:

- misure organizzative: istruzioni impartite agli operatori (blocco della postazione, spegnimento ordinato all'uscita, divieto d'installazione di software non autorizzato, etc.)
- misure tecniche: antivirus, aggiornamenti di sistema operativo, etc.

L'accesso da rete pubblica è inibito per il computer utilizzato per la gestione dei dati personali. In ogni caso, l'accesso alla intranet aziendale è protetto da Multi-Factor Authentication (Cisco Duo).

6.13 Manutenzione

Per la parte di infrastruttura, la manutenzione del server fisico è demandata al personale IT del Titolare. In particolare, per parti impiantistiche sono previsti contatti di manutenzione ordinaria e straordinaria con outsourcer specifici, mentre per la parte di apparati e sistemi di elaborazione, una volta scaduta la garanzia, sono sottoscritti appositi contratti di manutenzione.

Per la postazione utilizzata, verrà disabilitata la possibilità di accesso VPN.

6.14 Contratto con il responsabile del trattamento

Il contratto con il responsabile del trattamento contiene opportune istruzioni e disciplina i rispettivi obblighi per assicurare la protezione dei dati personali.

6.15 Controllo degli accessi fisici

L'Ambulatorio dove è ubicata la postazione fissa utilizzata è accessibile solo a personale autorizzato. L'accesso all'ambulatorio da parte dei pazienti avviene soltanto per brevi periodi e sotto la supervisione del personale sanitario e infermieristico.

Per il datacenter sono implementate le seguenti procedure:

- Accesso solo a personale autorizzato
- Sistemi antiintrusione

6.16 Protezione contro fonti di rischio non umane

Per il Data Center sono previste le seguenti protezioni:

- Rilevazione fumi e spegnimento incendi. Tutti gli ambienti della sede sono dotati di rilevatori antifumo e antincendio con attivazione dei relativi impianti di spegnimento automatico degli incendi a saturazione di ossigeno. L'impianto di spegnimento è stato progettato nel pieno rispetto della normativa UNI 9795 che garantisce la segmentazione dell'impianto e di conseguenza la perdita delle sole zone oggetto di eventuale incidente o calamità naturale ed il continuo funzionamento del resto dell'impianto.
- Antiallagamento. Sono previste delle sonde di rilevazione presenza liquidi nel sottopavimento in prossimità dei raccordi, delle valvole e delle derivazioni principali dell'impianto di distribuzione dell'acqua e degli scarichi della condensa.
- Antintrusione. È attivo un sistema di antintrusione integrato con il sistema di Telecamere a circuito chiuso. Questo sistema protegge tutto il perimetro della sede, le aree comuni interne e gli impianti posti sul Lastrico Solare.
- I sensori del sistema allocati all'interno dell'edificio sono attivati e disattivati da segnali provenienti dal sistema di controllo accessi.
- Telecamere a circuito chiuso. Le telecamere sono posizionate per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche con il Lastrico Solare. Il sistema TVCC è predisposto per attivazione tramite "motion detection".
- Condizionamento: le condizioni di temperatura delle singole Computer Room sono regolate tramite termostati indipendenti situati nelle suddette Computer Room.
- Continuità ed Emergenza: sono presenti tre gruppi di continuità (UPS) centralizzati da 200 KVA ciascuno, operanti in parallelo. Gli UPS, in modalità N+1, assicurano la continuità a tutti i dispositivi informatici. Tali gruppi sono tenuti sotto monitoraggio 7x24.
- In caso di prolungata assenza di alimentazione elettrica vengono automaticamente attivati i due gruppi elettrogeni, in grado di garantire un'ampia autonomia di servizio.
- Alimentazione a 48 V. Le sale TLC sono equipaggiate con alimentazione a 48 V per gli apparati di telecomunicazione.
- Sistema monitoraggio alimentazioni elettriche. I quadri elettrici (impianti e sale) e gli interruttori dei singoli rack sono dotati di sensori collegati a sistema centralizzato per monitorare i consumi e generare alert su eventuali fault.
- Controllo degli accessi fisici all'IDC. Il personale che accede in nome e per conto dei Clienti è soggetto a procedure di registrazione degli accessi e identificazione del personale stesso.
- L'accesso alle sale sistemi è controllato elettronicamente tramite badge.
- Connettività: la connettività esterna per la raggiungibilità delle apparecchiature via rete pubblica (banda internet) o rete dedicata privata (rame o fibra ottica) è concentrata in apposita sala TLC. Attualmente presso i locali vi sono attestazioni di rete a Fibra Ottica dei principali fornitori di TLC (v. Telecom Italia, Fastweb, Wind)
- Sistema di gestione e remotizzazione allarmi. Gli eventuali allarmi rilevati sono registrati ed inoltrati anche a distanza per permettere di mantenere un costante controllo di tutta l'infrastruttura.

Il computer utilizzato è comunque collocato in uno stabile diverso rispetto all'ubicazione dei server, in cui la probabilità di allagamento è fortemente limitata.

6.17 Misure di sicurezza in caso di trasferimenti verso Paesi non adeguati

Non sono previsti trasferimenti al di fuori dello Spazio Economico Europeo.

6.18 Politica di tutela della privacy

Le politiche privacy del Titolare del trattamento e dei responsabili del trattamento, relative alla propria organizzazione, sono conformi al GDPR.

L'ASL TO5, al fine di garantire la conformità alla normativa in materia di protezione dei dati personali ha provveduto a costituire un Gruppo Operativo Privacy e a nominare, con determina dirigenziale n. 50 del 11/02/2021 quale DPO aziendale Liguria Digitale S.p.A. Il DPO dell'ASL TO5 ha un ruolo di verifica dei trattamenti nei confronti del Titolare del trattamento dati.

6.19 Gestione dei rischi

È stata effettuata la valutazione dei rischi i cui risultati sono nello specifico paragrafo.

6.20 Integrare la protezione della privacy nei progetti

La fase di progettazione ha tenuto conto dei requisiti di privacy by design.

6.21 Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Il Titolare ha adottato le seguenti procedure aziendali in materia di trattamento dei dati personali:
- Gestione delle violazioni di dati personali
- Gestione dell'esercizio dei diritti dell'interessato

Gli accordi in essere prevedono la collaborazione di tutti gli Enti coinvolti in caso di incidente.

6.22 Gestione del personale

L'ASL TO5, inoltre, con deliberazione n. 431 del 01/09/2020 ha individuato all'interno dell'organizzazione aziendali i Designati Privacy e gli Autorizzati al trattamento dati personali.

Il personale è stato formato con apposito corso FAD privacy e sistematicamente aggiornato.

6.23 Gestione dei terzi che accedono ai dati

Il soggetto terzo che ha accesso ai dati è il fornitore Dedalus Italia S.p.A. che offre un servizio di presidio e pertanto non accede dall'esterno della rete aziendale.

6.24 Vigilanza sulla protezione dei dati

Il Titolare ha nominato un DPO con il compito di vigilare sui trattamenti dei dati personali.

7. Fase 5: Consultazione degli interessati

Nello svolgimento della DPIA, il Titolare, valutate le specifiche circostanze del trattamento in esame, ha ritenuto non necessario e sconveniente provvedere alla raccolta delle opinioni dei soggetti interessati e dei rappresentati degli stessi.

Nelle specifiche circostanze non è stato possibile coinvolgere i soggetti interessati in quanto si tratta di soggetti difficilmente contattabili o deceduti.

8. Fase 6: Calcolo del rischio residuo, piano di remediation e parere del DPO

8.1 Rischio residuo

Si ritiene che il rischio residuo collegato al trattamento di dati personali per le finalità dello studio in oggetto sia accettabile in quanto sono state adottate misure di sicurezza tecniche e organizzative idonee a contenere il rischio per i diritti e le libertà degli interessati.

8.2 Piano di remediation

Per la minimizzazione del rischio residuo, non sono al momento previste ulteriori misure di sicurezza.

8.3 Opinione del DPO

L'indice di questo documento e relativi contenuti rispecchiano quanto indicato nell'allegato 2 del WP 248 *(Criteri per una valutazione d'impatto sulla protezione dei dati accettabile)* (cfr. Comitato Europeo per la protezione dei dati, Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248rev.01).
Il DPO, consultato dal Titolare in conformità all'art. 35, par. 2, del GDPR in merito alla Valutazione d'impatto ex artt. 35-36 GDPR (cd. DPIA) sulle attività di trattamento relative allo "Identificazione precoce del rischio di delirium nei pazienti ricoverati: validazione di uno score in Medicina Interna", nello svolgimento dei compiti attribuitigli, ha valutato che**:**

v. allegato

9. Fase 7: Eventuale consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR

Il trattamento dei dati personali rientra nei casi previsti dall'art. 110 del D.lgs 196/2003. Tale norma è stata, come indicato sopra, di recente modificata ad opera dell'art. 1, comma 1, della l. 29 aprile 2024, n. 56. di conversione del D.L. 2 marzo 2024, n. 19, eliminando l'obbligo di sottoporre la valutazione d'impatto alla consultazione preventiva dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR, e prevedendo che il Garante adotti misure a garanzia ai sensi dell'articolo 106, comma 2, lettera d), del D.lgs 196/2003.
Tale obbligo, pertanto, sussiste nelle ipotesi tipizzate dall'art. 36 GDPR, e dunque laddove il rischio residuo sia elevato. Come risulta dalla valutazione del rischio, e del calcolo del rischio residuo come sopra riportato, esso può individuarsi come accettabile, e dunque non si rientra in tale fattispecie.

10. Fase 8: Monitoraggio e riesame nel tempo della DPIA

Ai sensi del paragrafo 11 dell'art. 35 del GDPR, il Titolare deve:

- verificare che il trattamento dei dati personali sia effettuato conformemente alla DPIA. A tal fine il DPO effettuerà degli audit con cadenza annuale;
- procedere a un riesame del trattamento oggetto di DPIA quando vengono apportate modifiche al trattamento con conseguente variazione del livello di rischio connesso al trattamento stesso, al fine di valutare la necessità di apportare revisioni al DPIA Report ovvero di effettuare una nuova DPIA.

Per valutare se il livello di rischio è variato, si dovrà verificare se sono stati modificati uno o più dei seguenti aspetti:

- Cambiamento sulle attività di trattamento, in termini di:
  - contesto (variazione della localizzazione fisica o di elementi ambientali dell'azienda, nuovi vincoli, funzioni e struttura organizzativa, innesto di politiche e processi aziendali, leggi, norme e contratti);
  - modalità di raccolta dei dati personali (mediante modulo cartaceo o form elettronico, direttamente dall'interessato o indirettamente da terzi)
  - finalità del trattamento;
  - tipologia di dati personali trattati (ad esempio dati genetici);
  - categorie di interessati;
  - soggetti coinvolti nel trattamento (personale interno all'organizzazione o fornitori esterni);
  - combinazioni di dati (integrazione con dati provenienti da altre sorgenti, correlazione di informazioni censite su diverse basi dati);
  - trasferimento di dati all'estero (all'interno della UE o verso paesi od organizzazioni internazionali al di fuori della UE).

- Modifica ai rischi con impatti sui diritti e le libertà delle persone fisiche, derivanti da:

  - Modifica dei sistemi informativi a supporto (subentro di un nuovo Service Provider, migrazione di servizi in Cloud, ecc.);
  - nuovi scenari di rischio (furti di identità e frodi informatiche, introduzioni di attacchi avanzati e azioni non autorizzate)
  - insorgenza di potenziali impatti sulle qualità di riservatezza, integrità e disponibilità dei dati personali;
  - nuove minacce (naturali, ambientali, tecniche, di terrorismo o sabotaggio, provenienti da comportamenti volontari o accidentali);
  - attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali;
  - dismissione di elementi di presidio esistenti.

- Mutamenti nel contesto organizzativo o sociale per l'attività di trattamento, ad esempio perché gli effetti di determinate decisioni automatizzate sono diventati più significativi oppure perché nuove categorie di interessati sono diventati vulnerabili alla discriminazione.

A seguito delle predette verifiche dovrà essere calcolato il livello di rischio (utilizzando la procedura di cui al punto 7) e acquisito il parere del DPO in merito alla necessità di aggiornare la DPIA ovvero procedere ad una nuova valutazione d'impatto.

In ogni caso, anche a prescindere da modifiche apportate al trattamento, quest'ultimo sarà oggetto di riesame annuale, al fine di verificate se, a seguito di cambiamenti nelle conoscenze tecnico-scientifiche, si sia modificato il livello di rischio e sia quindi necessario adottare misure tecnico organizzative nonché rivedere/integrare la DPIA al fine di mantenere la validità e l'aggiornamento nel tempo della valutazione condotta e dei suoi risultati.

Elenco allegati:

Allegato 1-Elenco variabili;
Allegato 2 – Informativa privacy.;