FRONTESPIZIO PROTOCOLLO GENERALE

AOO: ASL_BO

REGISTRO: Protocollo generale

NUMERO: 0092615

DATA: 29/08/2023

OGGETTO: Risposta a richiesta di parere su Valutazione impatto sul trattamento dati personali (DPIA) relativa allo Studio Osservazionale Monocentrico Prospettico e Retrospettivo dal titolo: "Migrazione e urgenze psichiatriche: uno studio di coorte naturalistico"

SOTTOSCRITTO DIGITALMENTE DA:

Federica Filippini

CLASSIFICAZIONI:

- [01-07-08]

DOCUMENTI:

File	Firmato digitalmente da	Hash
PG0092615_2023_Lettera_firmata.pdf:	Filippini Federica	6A4E915F64CE374D165F80AF168D1A4E0CB2020B1CE7158B1ACDFE57280086DC
PG0092615_2023_Allegato1.pdf:		814E508447AA8DF89D058F4EBEA03CC0BDC82C3C6330E2ABBBC944491F412812

UO Affari Generali e Legali (SC)

Ilaria Tarricone - UO Diagnosi e Cura Malpighi (SS)

OGGETTO: Risposta a richiesta di parere su Valutazione impatto sul trattamento dati personali (DPIA) relativa allo Studio Osservazionale Monocentrico Prospettico e Retrospettivo dal titolo: "Migrazione e urgenze psichiatriche: uno studio di coorte naturalistico"

In riscontro alla richiesta di parere pervenuto il 24/08/2023 prot. 91339 al fine di dare attuazione alle indicazioni previste dall'art. 35 del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (GDPR) relativamente alla effettuazione della valutazione di impatto del trattamento (Data Protection Impact Assessement - DPIA) previsto sulla protezione dei dati personali si trasmette il parere di competenza espresso di seguito.
Nel novero delle tipologie previste dall'art. 35 del GDPR e in relazione all'elenco delle tipologie di trattamenti di cui al Provvedimento dell'Autorità Garante n. 467 dell'11 Ottobre 2018, il trattamento in questione ricade tra *i 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" ed è svolto, tra l'altro, utilizzando metodiche e tecnologie innovative di calcolo computazionale.
Al fine di ottemperare agli adempimenti derivanti dalla normativa in vigore si raccomanda di tener presenti le raccomandazioni descritte al punto 9.1 del documento della DPIA allegato alla presente nota e in particolare:

- assicurare quanto più possibile la comprensione e la divulgazione dell'informativa agli interessati;
- verificare periodicamente che predisposizione delle misure tecniche ed organizzative siano conosciute, osservate ed adeguate, in relazione alla peculiarità del trattamento, ivi compresi eventuali nuovi rischi.

Dato atto che la liceità del trattamento è da rinvenirsi nel consenso espresso così come previsto dall'art. 6 paragrafo 1 lett. a e fronte delle misure tecniche e organizzative predisposte, il rischio per i diritti e le libertà degli interessati può essere classificato BASSO, in conformità alle disposizioni di cui all'art. 39, lettera c del su citato Regolamento, la scrivente UO avendo analizzato il contenuto della valutazione d'impatto eseguita, esprime parere favorevole al trattamento dei dati personali che verrà effettuato nell'ambito dello Studio "Migrazione e urgenze psichiatriche: uno studio di coorte naturalistico"

Firmato digitalmente da:

Federica Filippini

Responsabile procedimento:
Federica Filippini

U.O. Data Protection Officer
IRCCS Azienda Ospedaliero Universitaria di Bologna
Ausl di Bologna
Ausl di Imola
Istituti Ortopedici Rizzoli
Montecatone Rehabilitation Institute

Azienda USL di Bologna
Sede legale: via Castiglione, 29 - 40124 Bologna
Tel +39.051.6225111 fax +39.051.6584923
Codice fiscale e partita Iva 02406911202

VALUTAZIONE D'IMPATTO
SULLA PROTEZIONE DEI DATI DPIA
STUDIO OSSERVAZIONALE MONOCENTRICO PROSPETTICO E RETROSPETTIVO

Promotore: Azienda USL di Bologna – IRCCS ISNB
Sperimentatore principale: Dr.ssa Ilaria Tarricone
Centro sperimentale: Servizio psichiatrico diagnosi e cura Area EST "SPDC-Malpighi", Servizio Psichiatrico di Diagnosi e Cura Distretto Pianura Area Ovest "SPDC San Giovanni in Persiceto", Unità Operativa Semplice - Centro di Salute Mentale "UOS - CSM Savena – Santo Stefano", Azienda USL di Bologna

NOME DEL PROGETTO:	Migrazione e urgenze psichiatriche: uno studio di coorte naturalistico
DESCRIZIONE DEL PROGETTO:	Il presente progetto di ricerca si propone di valutare le variabili socio-demografiche pre/post-migrazione e le caratteristiche della storia migratoria dei pazienti migranti di prima e seconda generazione e nativi ricoverati e afferenti presso SPDC Malpighi, CSM Savena-Santo Stefano e SPDC San Giovanni in Persiceto. Lo studio si propone inoltre di individuare i fattori correlati all'attuazione degli accertamenti e dei trattamenti sanitari obbligatori nei Servizi di salute mentale coinvolti, esplorando la correlazione tra dimensioni organizzative e strutturali dei suddetti Servizi, l'atteggiamento verso la coercizione da parte degli operatori, numerosità e caratteristiche di TSO e ASO.

Responsabile elaborazione DPIA:	**Funzione/Ruolo aziendale:**
Team Multidisciplinare	
Prof.ssa Ilaria Tarricone	Ricercatore principale/ Porfessore associato equiparato a Dirig. Medico – Psichiatra, UO Diagnosi e Cura Malpighi (SS)
Dott.ssa Margherita Alfieri Dott. Francesco Maria Fasulo	Team ricerca/medici in formazione specialistica in psichiatria, SPDC Malpighi
Funzioni Privacy	UO Affari Generali e Legali

Sommario

Definizioni e Abbreviazioni

CSM	Centro di Salute Mentale
SPDC	Servizio Psichiatrico di Diagnosi e Cura
DSM	Dipartimento di Salute Mentale
ASO	Accertamento Sanitario Obbligatorio
TSO	Trattamento Sanitario Obbligatorio
CRF- BMH&SI	Case Record Form Bologna Migration History and Social Integration
SACS	Staff Attitude to Coercion Scale
CCE	Cartella Clinica Elettronica

Sezione 0 - Verifica preliminare di applicabilità della DPIA (Valutazione di impatto), in conformità all'articolo 35, del Regolamento Generale sulla protezione dei dati – Regolamento (UE) 2016/679 - GDPR

***Verificare se il trattamento coinvolto, dopo essere stato assoggettato all'analisi di rischio, può ricadere in uno dei casi previsti, per i quali è obbligatoria la conduzione di una DPIA* (Data Protection Impact Assessment)[1]**

- ✓ Il trattamento ricade tra quelle tipologie di trattamento inserite nell'elenco pubblico dell'Autorità Garante Nazionale (ex Art. 35 p. 4 GDPR - Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018) che richiedono specificamente lo sviluppo di una DPIA;
- ✓ Il trattamento coinvolto ricade in uno dei casi per i quali la conduzione della DPIA è obbligatoria: Art. 35 p. 3 lett. B GDPR "il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1".

Data di avvio della DPIA: 15/06/2023

Sezione 1 - Avvio della valutazione

1.1 Tipologia di progetto [2]
Studio retrospettivo e prospettico, osservazionale e monocentrico, non interventistico, non farmacologico e non commerciale.

1.2 Valutazione preliminare dell'utilizzo dei dati [3]
1.2.2 Come verranno raccolti i dati?
I dati, per la parte retrospettiva dello studio (relativi ai pazienti), verranno raccolti dai database sanitari (CURE) e dalle cartelle cliniche (CCE) e dal registro contenzioni. I dati, per la parte prospettica dello studio verranno raccolti: per il personale dipendente: mediante intervista di ricerca (scheda sociodemografica, clinica e sulla storia migratoria "SACS - Staff Attitude to Coercion Scale"; per i pazienti: mediante intervista di ricerca "Case Record Form e Bologna Migration History and Social Integration". Un numero di identificazione univoco verrà assegnato a ciascun soggetto interessato (paziente e dipendente) al fine di riportarne i

[1] in alcune tipologie di trattamento può essere raccomandata la conduzione di una valutazione di impatto, anche se il trattamento in questione non risulta fra quelli per i quali tale valutazione è obbligatoria.

[2] esaminare le finalità del progetto in modo da esser certi di conoscere gli obiettivi e l'impatto potenziale. Se esiste un documento introduttivo o esplicativo cui fare riferimento, coinvolgere i referenti del progetto.

[3] rispondere alle domande seguenti in modo che vi sia una chiara comprensione di come le informazioni verranno utilizzate. Se non si è in grado di rispondere a tutte le domande, scrivere almeno ciò che si conosce.

rispettivi dati nella eCRF.
Presso il centro sarà tenuto un elenco di identificazione che collega il numero di identificazione all'identità dell'interessato.

1.2.3 Chi avrà accesso ai dati?

Lo sperimentatore principale (Prof.ssa Ilaria Tarricone) ed i suoi collaboratori: Dott.ssa Margherita Alfieri, Dott. Francesco Maria Fasulo, Dott.ssa Caterina Bruschi, Dott.ssa Angela Trappoli, Dott. Federico Chierzi e Dott.ssa Catia Nicoli, sono gli unici autorizzati ad accedere ai dati dei soggetti coinvolti nel progetto di studio.

1.2.4 In che modo i dati verranno eventualmente comunicati a soggetti terzi?

I dati potranno essere comunicati alle Autorità Regolatorie competenti, al Comitato etico indipendente di area vasta Emilia centro (CE-AVEC) e alle autorità sanitarie italiane che potranno esaminare tutta la documentazione sanitaria dell'Interessato raccolta nel corso dello studio: lo scopo di queste verifiche è controllare che la ricerca sia condotta correttamente e in conformità alle disposizioni vigenti.
Si precisa che i dati saranno diffusi solo in forma rigorosamente anonima e aggregata, ad esempio attraverso pubblicazioni scientifiche, statistiche e convegni scientifici.

1.3 Analisi preliminare dei soggetti coinvolti [4]

Promotore dello studio: AUSL Bologna

Centro sperimentale: Servizio psichiatrico diagnosi e cura Area EST "SPDC-Malpighi", Servizio Psichiatrico di Diagnosi e Cura Distretto Pianura Area Ovest "SPDC San Giovanni in Persiceto", Unità Operativa Semplice - Centro di Salute Mentale "UOS - CSM Savena – Santo Stefano", Azienda USL di Bologna

Steering Committee:
Prof.ssa Ilaria Tarricone
Dott.ssa Caterina Bruschi - UO Centro di Salute Mentale Savena-Santo Stefano. Azienda Unità Sanità Locale, Bologna
Dott.ssa Catia Nicoli - Dott. Federico Chierzi - UO Servizio Psichiatrico di Diagnosi e Cura San Giovanni in Persiceto. Azienda Unità Sanitaria Locale, Bologna
Dott.ssa Margherita Alfieri - Dott Francesco Maria Fasulo – Dott. Oscar Mordenti - Scuola di specializzazione in

[4] inserire coloro che sono coinvolti nel progetto e/o coloro che potrebbero essere coinvolti, anche indirettamente. È meglio compilare una lista la più ampia possibile, che potrà essere ridotta successivamente, quando l'indagine diventerà sempre più focalizzata.

Psichiatria, Università degli Studi di Bologna

1.4 Analisi di contesti precedenti e similari [5]
Non presenti

Sezione 1 completata da:	**Data:**
Team multidisciplinare	15/06/2023

Sezione 2 - Impostazione dell'analisi di rischio preliminare [6]

2.1 Tecnologie utilizzate

2.1.1 In questo progetto verranno utilizzate nuove tecnologie informatiche che potrebbero avere un significativo potenziale di violazione della protezione dei dati personali e riduzione del livello di protezione dei dati, che bisogna garantire agli interessati?
No

2.2 Metodi di identificazione

2.2.1 Verranno utilizzati nuovi metodi di identificazione dei dati o verranno riutilizzati identificatori già esistenti ed in uso?
L'identificazione dei soggetti interessati avverrà mediante identificatori esistenti già in uso. Successivamente, a ciascun soggetto arruolato verrà assegnato un codice univoco alfanumerico.

2.2.3 Verranno utilizzati nuovi o significativamente modificati requisiti di autentica di identità, che possono risultare intrusivi od onerosi?
No

2.3 Coinvolgimento di altre strutture

2.3.1 Questa iniziativa di trattamento coinvolge altre strutture, sia pubbliche, sia private, sia appartenenti a settori non-profit e volontari?
No

2.4 Modifiche alle modalità di trattamento dei dati

2.4.1 Questa iniziativa di trattamento apporterà nuove o significative modifiche alle modalità di trattamento dei dati personali, che potrebbero destare preoccupazioni nell'interessato? [7]

[5] in questa fase è opportuno raccogliere informazioni su progetti precedenti, di natura similare, sviluppatisi all'interno, sia all'esterno dell'ente.

[6] una analisi di rischio è sempre necessaria, per decidere se una DPIA è obbligatoria o raccomandata

[7] verificare se le modifiche potrebbero riguardare le origini razziali ed etniche, le opinioni politiche, i dati sanitari, la vita sessuale, trascorsi giudiziari, tali da comportare un rischio reale per i diritti e le

No. In generale, non si ritiene che questa iniziativa di trattamento possa destare delle preoccupazioni nei soggetti interessati posto che le finalità dello studio sono rese esplicite in quanto dichiarate nell'informativa sul trattamento dei personali ex art. 13 GDPR nonché nella documentazione predisposta per il progetto e approvata dal competente comitato etico.

2.4.2 I dati personali, propri di un interessato, già presenti in un esistente data base, verranno assoggettati a nuove o modificate modalità di trattamento?

Sia per la parte retrospettiva che per quella prospettica dello studio, i dati riferibili ai pazienti, vengono estratti da cartelle cliniche e data base sanitari (raccolti nel contesto della primaria attività di cura) ed riutilizzati per finalità di ricerca scientifica.

2.4.3 I dati personali, propri di un gran numero di interessati, verranno assoggettati a nuove o significative modifiche delle modalità di trattamento?

Sì, i dati dei soggetti coinvolti (circa 1200 pazienti e 100 operatori) verranno trattati con nuove modalità per finalità di ricerca scientifica.

2.4.4 Questa iniziativa di trattamento apporterà nuove o significative modifiche alle modalità di consolidamento, interscambio, riferimenti incrociati, abbinamento di dati personali, provenienti da più sistemi di trattamento?

No

2.5 Modifiche alle procedure di trattamento dei dati

2.5.1 Questo trattamento potrà introdurre nuove modalità e procedure di raccolta dei dati, che non siano sufficientemente trasparenti o siano intrusive?

Per ciò che attiene alla parte retrospettiva dello studio, non è presente un'inziale fase di raccolta, dal momento che si selezionano ed utilizzano dati personali già presenti in cartelle cliniche e data base sanitari.
Trattasi, pertanto, di dati raccolti per finalità diverse ed ora sottoposti ad un nuovo trattamento (ricerca) e il cui riutilizzo richiede uno specifico consenso da parte degli interessati.
Per la parte prospettica (in particolare mediante l'utilizzo dell'intervista strutturata), non si ritiene che si introducano modalità e procedure di raccolta dei dati non sufficientemente trasparenti o intrusive poiché le stesse sono state dichiarate nell'informativa e nei documenti predisposti per il progetto di ricerca (es. Protocollo di studio, consenso informato).

2.5.2 Questo trattamento potrà introdurre modifiche a sistemi e processi, costruiti in conformità a normative in vigore, che possano avere esiti non chiari o non

libertà l'interessato.

soddisfacenti?
Non si ritiene che questo trattamento possa introdurre modifiche a sistemi e processi, costruiti in conformità a normative in vigore, che possano avere esiti non chiari o non soddisfacenti poiché lo studio verrà svolto in conformità: - alle norme in materia di consenso informato e di disposizioni anticipate di trattamento (di tipo sanitario); - alle norme in materia di protezione dei dati personali.

2.5.3 Questo trattamento potrà introdurre modifiche a sistemi e processi, che modifichino il livello di sicurezza dei dati, in modo da portare ad esiti non chiari o non soddisfacenti?
No, in quanto verranno adottate tutte le misure tecniche e organizzative necessarie a garantire la sicurezza dei dati personali oggetto del trattamento.

2.5.4 Questo trattamento potrà introdurre nuove o modificate procedure sicure di accesso ai dati o modalità di comunicazione e consultazione non chiare o permissive?
No, l'accesso ai dati nonché la consultazione degli stessi verranno eseguite mediante procedure preesistenti e regolamentate nelle policy aziendali.

2.5.5 Questo trattamento introdurrà nuove o modificate modalità di conservazione dei dati non chiare o prolungate oltremodo?
Per come è strutturato il percorso di conservazione dei dati (10 anni dal termine dello studio), non si ritiene che questo possa definirsi prolungato poiché è quello strettamente necessario per il raggiungimento degli obiettivi del progetto. I tempi di conservazione sono stati descritti nella documentazione dello studio.

2.5.6 Questo trattamento modificherà le modalità di messa a disposizione dei dati?
No

2.6 Esenzioni dalla applicazione delle disposizioni del regolamento – art.2 comma 2[8]

2.6.1 L'attività di trattamento esula dall'ambito delle disposizioni legislative dell'Unione Europea?
No

2.6.2 Il trattamento è svolto da una persona fisica esclusivamente per fini personali e familiari? In questo caso è anche consentita la diffusione di dati personali che saranno accessibili solo ad un limitato numero di persone,

[8] l'articolo 2 del GDPR prevede alcune esenzioni al campo di applicabilità del regolamento stesso

come i familiari e conoscenti?
N/A

2.6.3 L'attività di trattamento è svolta da autorità pubbliche al fine di prevenzione, indagine, individuazione e perseguimento di reati o al fine di applicare pene?
N/A

2.7 Giustificazioni per l'avvio del progetto di trattamento

2.7.1 Le giustificazioni per l'avvio del trattamento includono contributi significativi ad implementare misure in grado di migliorare il livello della sicurezza pubblica?
No

2.7.2 Si prevede di effettuare una consultazione pubblica?
No

2.7.3 Le finalità di trattamento dei dati sono chiare e sufficientemente pubblicizzate?
Le finalità del trattamento sono descritte nel contesto della sinossi e del Protocollo di Studio, valutati dal Comitato Etico dell'Area Vasta Emilia Centro nonché dichiarate nell'informativa sul trattamento dei dati personali ex art. 13 GDPR, resa ai soggetti coinvolti.

Sezione 2 completata da: TEAM multidisciplinare	**Data:** 27/06/2023

Sezione 3 - Esito dell'analisi preliminare dei rischi

3.1 Identificazione preliminare dei rischi [9]
La tabella seguente illustra i principali rischi afferenti alla protezione dei dati, che sono stati identificati in fase di valutazione preliminare

	Descrizione del rischio	**Valutazione preliminare di esposizione** [10]
Rischio 1	**Distruzione**	**Basso**
Rischio 2	**Perdita**	**Basso**
Rischio 3	**Distribuzione non autorizzata**	**Medio**
Rischio 4	**Accesso ai dati non autorizzato**	**Medio**

[9] a questo stadio non è ancora opportuno fare una valutazione dettagliata di tutti i rischi, ma prima di procedere con la DPIA è bene aver correttamente identificato i rischi principali.

[10] si raccomanda di fare riferimento la normativa europea ISO EN 31000, che classifica i rischi e i cinque livelli, dal primo livello-accettabile, sino al quinto livello-catastrofico.

Rischio 5	**Trattamento non autorizzato**	**Medio**
Rischio 6	**Trattamento non conforme alla finalità della raccolta o illecito**	**Basso**

3.2 Decisione su come procedere
Sulla base delle informazioni finora raccolte e sugli adempimenti prescritti dalla normativa vigente si decide di proseguire con la redazione della DPIA.

Nome di colui che ha assunto la decisione [11]	Team multidisciplinare
Nome di altri soggetti che hanno condiviso questa decisione	N/A

Sezione 3 completata da TEAM multidisciplinare	**Data:** 27/06/2023

Sezione 4 - Preparazione per la fase di consultazione ed analisi

4.1 Disposizioni afferenti alla Governance[12]
Questo documento verrà gestito come parte integrante del Protocollo di Studio. I soggetti appartenenti al team di ricerca verranno coinvolti nell'elaborazione della presente DPIA.

4.2 Altri soggetti eventualmente coinvolti, da consultare[13] -
Non presenti

Soggetto terzo: nome/ organizzazione/ ruolo	**Quale interesse ha questo soggetto terzo in questo progetto di trattamento?**	**Con quali modalità viene sviluppata la consultazione con questo soggetto?**
N.A.		

Soggetti interni coinvolti		
Vedasi punto 1.3		

4.3 Strategia di consultazione [14]

[11] il data controller è il soggetto che ha la responsabilità finale della decisione.
[12] scegliere tra le due la risposta più appropriata per completare la tabella. Aggiungere altri nomi e funzioni secondo necessità.
[13] questa parte fa riferimento a quanto già sviluppato al punto 1 per identificare i soggetti terzi coinvolti. È appropriato valutare con maggior dettaglio quali sono gli interessi dei vari soggetti terzi coinvolti e il loro coinvolgimento nello sviluppo della DPIA. Non elencare questi soggetti terzi se fanno già parte del team di progetto o di un team separato coinvolto nell'elaborazione della DPIA.
[14] se già viene attuata una strategia di consultazione, afferente a questo progetto, non è necessario elaborarne una separata per lo sviluppo della DPIA. Occorre tuttavia essere certi che questa strategia di

N/A

4.4 Risorse [15]
Non sono necessarie ulteriori risorse umane ed economiche

4.5 Consultazione preventiva [16]
Non si ritiene che il trattamento comporti un elevato livello di rischio tale da attivare il procedimento di consultazione preventiva ex art. 36 GDPR.

Sezione 4 completata da	**Data:**
TEAM multidisciplinare	31/07/2023

Sezione 5 - Consultazione [17]

5.1 Soggetti terzi coinvolti
N/A (vedasi p.4.2)

Nome del soggetto coinvolto	

5.2 Soggetti interni coinvolti [18]
Non presenti

Nome del soggetto coinvolto	**Illustrazione di eventuali osservazioni avanzate in fase di consultazione**

Sezione 6 - Congruità con altre leggi, codici o regolamenti afferenti alla protezione dei dati [19]

6.1 Indicazione normativa e provvedimenti
✓ Regolamento (UE) 2016/679;

consultazione tocchi tutti gli aspetti di protezione dei dati del progetto quindi spiegare in dettaglio che approccio viene adottato.

[15] si effettua una valutazione circa la necessità di risorse ulteriori (umane o economiche), per sviluppare in modo efficace la DPIA.

[16] se l'analisi preventiva ha messo in evidenza che le operazioni di trattamento possono presentare un elevato livello di rischio, occorre contattare l'Autorità Garante, secondo quanto indicato all'articolo 34 del GDPR.

[17] per DPIA che prevedono il trattamento di dati su larga scala ricordarsi di completare sempre la sezione 6 per essere certi di svolgere un'attività congrua con il regolamento e altre disposizioni legislative in tema di protezione dei dati.

[18] si faccia attenzione a non inserire in questo elenco coloro che fanno parte del team che deve elaborare il documento in questione. Vanno inserite UO o Dipartimenti che per svolgere la loro attività hanno evidentemente necessità di accedere e trattare dati personali.

[19] elencare di seguito tutti i provvedimenti legislativi o regolamentari che si applicano alla specifica attività di trattamento ipotizzata; non dimenticare eventuali codici etici od associativi. In particolare, l'articolo 42 del GDPR fa specifico riferimento a codici di condotta applicabili a specifiche modalità di trattamento. Si raccomanda di leggere attentamente l'articolo 38, onde illustrare il provvedimento e le misure adottate per soddisfare le indicazioni, sia vincolanti, sia orientative, del provvedimento stesso.

- ✓ D.lgs. 30 giugno 2003, n. 196 recante “Codice in materia di protezione dei dati personali”;
- ✓ D.lgs. 10 agosto 2018, n. 101 recante “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679;
- ✓ Le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica adottate dal Garante, ai sensi dell’art. 20, comma 4, del d.lgs. 10 agosto 2018, n.101, con provvedimento n. 515, del 19 dicembre 2018 (doc. web n. 9069637);
- ✓ Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, allegati 4 e 5 al provvedimento del 5 giugno 2019 (doc. web 9124510).

In relazione alla normativa e provvedimenti sopra elencati, è stata effettuata una verifica di conformità, come parte di questa DPIA, secondo quanto illustrato nella appendice A e siamo giunti alla seguente conclusione: non si ritiene che il trattamento comporti un elevato livello di rischio tale da attivare il procedimento di consultazione preventiva all’Autorità Garante.

Sezione 7 - Contenuti analitici della DPIA [20]

Fare riferimento alla appendice B laddove sono illustrati tutti i rischi identificati e illustrate le opzioni che permettano di mitigare, evitare o mettere sotto controllo questi stessi rischi

7.1 Descrizione analitica delle operazioni di trattamento, con indicazione delle finalità e dei legittimi interessi perseguiti dal Titolare del Trattamento

7.2 Valutazione della necessità e proporzionalità delle operazioni di trattamento, in relazione alle finalità

I dati trattati seguono un Protocollo di Studio che ne definisce gli obiettivi e il disegno, conseguentemente definisce i limiti e gli ambiti di trattamento di tali dati. Secondo quanto previsto nel progetto, vengono raccolte, catalogate e analizzate esclusivamente le informazioni strettamente necessarie per la finalità dello studio. Ne consegue che i soggetti autorizzati ad analizzare i dati, andranno a selezionare/raccogliere e trattare solamente dati già preventivamente concordati e per il tempo strettamente necessario alla finalità perseguita.

7.3 Valutazione dei rischi che incidono sui diritti e le libertà degli interessati, incluso il rischio di discriminazione connesso o rinforzato dal trattamento

Si rimanda all’Appendice B.

7.4 Descrizione delle misure individuate per mettere sotto controllo i rischi e ridurre al minimo il volume di dati

[20] l’articolo 35, punto 7, elenca in forma analitica tutte le voci che debbono comporre la DPIA

personali da trattare - Data Protection by Default [21]

All’interno del Protocollo sono state identificate le categorie dei dati personali da trattare e sono implementate misure che consentono di raccogliere esclusivamente tali dati e solo quelli relativi ai pazienti effettivamente inclusi, in modo da rispondere al principio di minimizzazione.

7.5 Elenco dettagliato delle salvaguardie, delle misure di sicurezza e dei meccanismi adottati per garantire la protezione dati personali, come ad esempio la pseudonimizzazione, oppure la crittografia, al fine di dimostrare la congruità con il regolamento, tenendo conto dei diritti e dei legittimi interessi degli interessati ed altre persone coinvolte

Accesso ai dati riservato

L'accesso ai sistemi contenenti dati personali (PC, cartelle condivise, database etc.) avviene tramite codice ID e password, attribuiti a ciascun utente univocamente e individualmente.

Gli strumenti di autenticazione (password) sono comunicate agli utenti in modo tale che sia mantenuta la loro riservatezza e non vengono comunicate o usate da altri utenti.

Le password sono cambiate periodicamente, è richiesta una lunghezza minima (almeno otto caratteri oppure un numero di caratteri pari al massimo consentito dal sistema) e devono contenere almeno due tipologie diverse di caratteri (ad es. lettere, numeri, caratteri speciali, maiuscoli etc.)

Esistono autorizzazioni specifiche per diversi utenti o categorie di utenti, limitando l'accesso ai soli dati strettamente necessari per l'espletamento delle attività. Sono limitati e controllati l'assegnazione e l'uso di diritti di accesso privilegiato.

Esiste un processo strutturato e formalizzato che prevede la creazione, modifica e cancellazione degli utenti in caso di inizio, cambio o cessazione del rapporto di lavoro o delle mansioni

Periodicamente avviene la rivisitazione dei diritti di accesso degli utenti e viene verificato periodicamente l'effettivo allineamento tra ID/account attivi e utenti autorizzati.

Il sistema centrale è dotato di un SW/sistemi di alert che identifica e registri su log ogni tentativo di effrazione

Pseudonimizzazione

Un numero di identificazione univoco verrà assegnato a ciascun soggetto interessato coinvolto, al fine di riportarne i rispettivi dati nella eCRF e nei documenti cartacei.

Presso il centro sarà tenuto un elenco di identificazione che collega il numero di identificazione all'identità dell’interessato.

Sono definite modalità, circostanze e persone autorizzate per risalire all'identità dell’interessato.

Gestione postazioni - le postazioni utilizzate sono in dominio aziendale e le misure adottate sono quelle previste da regolamenti e policy aziendali. I dispositivi esterni e personali non possono ottenere l’accesso all’intranet aziendale.

[21] Nota: si prenda buona nota anche del fatto che questo tema viene trattato nella DPbD

Controllo degli accessi fisici - I locali (edifici, siti, stanze...) sono protetti tramite controlli d'accesso meccanici (cancelli, sbarre, etc.) e controlli d'accesso elettronici (badge) I locali sono chiusi a chiave e le chiavi/badge d'accesso sono disponibili solo al personale autorizzato.

Sicurezza dei documenti cartacei - in base alle istruzioni generali impartite dal Titolare, ogni singolo soggetto coinvolto nello specifico progetto di ricerca, condivide la documentazione prodotta con i soli appartenenti all'equipe di ricerca. Normalmente la documentazione cartacea riguarda i dati del progetto (es. Protocollo, parere del Comitato etico), poiché i dati personali relativi ai soggetti coinvolti vengono trattati principalmente in modalità informatizzata. Gli uffici dispongono di armadi con chiusura a chiave, accessibili solo dal personale autorizzato.

Sicurezza dei canali informatici - tutte le postazioni e i dispositivi aziendali sono equipaggiati con strumenti di antispam, antivirus, sonde di monitoraggio del traffico, sistemi di monitoraggio degli apparati fisici di rete e server e gestione degli alert. La difesa perimetrale della rete viene assicurata dalla separazione logica della stessa e dal posizionamento opportuno di firewall tra ambiti diversi.

Gestione delle politiche di tutela della privacy - Il Titolare ha adottato Privacy Policy aziendali periodicamente revisionate, disponibili su sito web aziendale e condivise con tutto il personale.
Il personale viene adeguatamente formato in merito alle attività di trattamento e alle misure di sicurezza da adottare:
- sono redatti specifici regolamenti interni;
- vengono effettuate sessioni formative.

7.6 Indicazione generale dei limiti di tempo per procedere alla cancellazione delle diverse categorie di dati raccolti

Il termine previsto è 10 anni dalla conclusione dello studio. Alla scadenza del termine i dati saranno cancellati o comunque resi anonimi.

7.7 Illustrazione di quali procedure di data protection by design e data protection by default verranno adottate, in conformità all'articolo 32 GDPR

Vedasi punto 7.4

7.8 Elenco dei destinatari o delle categorie di destinatari dei dati personali

PI e Staff del PI oltre ai Professionisti indicati nel delegation log

7.9 Se applicabile, fare elenco nominativo dei trasferimenti previsti dei dati verso paesi terzi o organizzazioni internazionali[22]

N/A

7.10 Verificare che il trasferimento verso paesi terzi od organizzazioni internazionali rispetti le modalità previste o

[22] nel caso il trasferimento di dati fare riferimento all'articolo 44 e documentare le appropriate misure adottate.

sia supportato da dichiarazioni di adeguatezza, emanate dalla Commissione Europea, la presenza di accordi internazionali, altre disposizioni o accordi contrattuali standard che legittimino il trasferimento
N/A

7.11 Valutazione del contesto del trattamento dei dati, presso paesi terzi
N/A

7.12 Eventuale coinvolgimento del DPO
Al fine di un confront che tenesse conto delle criticità insite nella peculiarità del trattamento il DPO è stato coinvolto fin dalla progettazione del percorso di ricerca, inoltre in osservanza della Del. n. 35559 del 12/10/2022 al DPO spetta validare il documento finale della DPIA e, conseguentemente, esprimere parere di competenza.

Sezione 8 - Revisione ed aggiornamento, con riesame di congruità con le esigenze di protezione dei dati -art 35 GDPR

8. Illustrazione del piano di revisione ed aggiornamento del data protection Impact assessment
La revisione della DPIA verrà effettuata tempestivamente nei casi specifici in cui è necessaria una azione correttiva o di miglioramento delle modalità di trattamento e comunque ogni tre anni.

8.1 Data entro la quale deve essere condotto il riesame di congruità
Il riesame sarà effettuato con cadenza triennale, tale periodo può variare in rapporto alle eventuali criticità rilevate durante le fasi del trattamento o a seguito di interventi normativi, regolatori, audit.

8.2 Nell'Intervallo di tempo trascorso tra il completamento della prima DPIA e la data entro la quale deve essere condotto il riesame, si sono evidenziate delle modifiche nei rischi connessi al trattamento?[23]
N/A in questa fase

8.3 Il riesame di congruità ha messo in evidenza delle anomalie?[24]
N/A in questa fase

8.4 Il riesame di congruità e le eventuali raccomandazioni sono state documentate per iscritto?[25]

[23] in caso di risposta affermativa, illustrare la situazione

[24] se la risposta è positiva, illustrare le indicazioni che permettono di raggiungere un soddisfacente livello di congruità;

N/A in questa fase

8.5 Il DPO è stato coinvolto nel riesame di congruità?
N/A in questa fase

Sezione 8 completata da: TEAM multidisciplinare	**Data:** 01/08/2023

Sezione 9 - Approvazione della DPIA

9.1 Raccomandazioni [26]
In considerazione della peculiarità del trattamento al fine di ottemperare agli adempimenti derivanti dalla normativa vigente si raccomanda di: • presidiare accuratamente le attività di raccolta dei dati e le misure adottate al fine di tutelare i diritti e libertà degli interessati; • assicurare quanto più possibile la comprensione e la divulgazione dell'informativa agli interessati; • verificare periodicamente che la predisposizione delle misure tecniche ed organizzative siano conosciute, osservate ed adeguate, in relazione alla peculiarità del trattamento, ivi compresi eventuali nuovi rischi.

9.2 Approvazione [27]
L'approvazione del presente documento tiene conto delle risorse umane e materiali disponibili. Non vi sono elementi critici che ne condizionano l'approvazione.

Sezione 9 completata da: TEAM multidisciplinare DPO	**Data:**	

Sezione 10 - Attivazione del trattamento [28]

Sezione 10 completata da: TEAM multidisciplinare	**Data:** 01/08/2023

[25] attenzione, questo documento deve essere disponibile all'Autorità Garante, in caso di audit o a richiesta.

[26] sulla base della analisi condotta fino a questo punto, indicate quali opzioni siete in grado di raccomandare per procedere. Se rimangono in evidenza rischi significativi, occorre illustrare quale sia il problema e perché fino adesso tale problema non è stato messo sotto controllo.

[27] sottolineare che la approvazione comporta anche la messa disposizione di appropriate risorse umane e materiali; è indispensabile indicare in questa casella chi ha approvato le raccomandazioni del punto 8.1 ed eventuali limitazioni e condizioni che hanno condizionato questa approvazione.

[28] illustrare di seguito quali controlli sono stati effettuati prima di avviare l'attività di trattamento, in modo da essere certi che le soluzioni di protezione dei dati approvate come parte di questa valutazione siano efficaci e che il sistema di trattamento sia pienamente conforme alle disposizioni normative.

Appendice A - Lista di controllo della congruità del trattamento previsto con le esigenze di protezione dei dati [29]

	Domanda	Risposta
1.	**Quali tipologie di dati personali vengono trattate?**	Vengono trattati dati di natura comune che permettono l'identificazione diretta ed indiretta dei soggetti arruolati e dati di natura particolare (dati relativi alla salute).
2.	**Sulla base di quanto illustrato nella DPIA, esiste una motivazione legittima per il trattamento?**	Il trattamento è motivato da fini di ricerca scientifica. La base giuridica del trattamento è il consenso dell'interessato - Art. 6, par. 1 lett. a), GDPR.
3.	**Se vengono trattati speciali categorie di dati, elencati all'articolo 9 comma 1 GDPR, sulla base di quanto illustrato nella DPIA, esiste una motivazione legittima per il trattamento?**	Il trattamento è motivato da fini di ricerca scientifica. La base giuridica del trattamento è il consenso dell'interessato - Art. 9, par. 2 lett. a), GDPR.
4.	**Vi sono aspetti afferenti al rispetto dell'articolo 2, comma 2, del regolamento, che protegge i diritti fondamentali e le libertà delle persone fisiche, ed in particolare il loro diritto alla protezione dei dati personali, che non siano trattati in questa DPIA?** [30]	NO
5.	**Tutti i dati personali che verranno trattati sono coperti da garanzie di riservatezza? Se sì, come viene garantita?**	Tutte le operazioni di trattamento sono effettuate da (o sotto la responsabilità di) un professionista sanitario, soggetto al segreto professionale
6.	**Come viene offerta agli interessati l'informativa in merito al fatto che i loro dati**	È previsto il rilascio dell'informativa direttamente ai soggetti

[29] se le risposte a queste domande sono state già date nella sezione 1 di questo documento, fate un riferimento incrociato all'appropriata risposta

[30] ricordarsi delle esenzioni previste per le finalità di sicurezza pubblica, indagini penali e simili

	personali verranno raccolti e trattati?	arruolati per lo studio. Per i soggetti che versano in uno stato clinico tale per cui sono impossibilitati a comprendere le indicazioni rese nell'informativa e a prestare validamente il consenso, tali informazioni saranno rese non appena le condizioni di salute lo consentano. Per i pazienti deceduti, come per quelli non ritracciabili, si prevede l'esenzione dall'obbligo di rendere l'informativa e della raccolta di consenso (motivi di impossibilità organizzativa) riconosciuta al punto 5 delle "Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016)", suddetti motivi sono descritti nella documentazione allegata al Protocollo di studio. Per i pazienti non rintracciabili, rimane fermo l'impegno del Centro a conferire l'informativa anche nel corso dello studio, nei casi in cui ciò sia possibile, laddove questi si rivolgano al centro di cura, anche per visite di controllo, anche al fine di consentire loro di esercitare i diritti previsti dal Regolamento.
7.	**Il progetto di trattamento dei dati comporta l'utilizzo di dati personali già raccolti, che verranno utilizzati per finalità secondarie?**	Sì, il progetto prevede in parte l'assoggettamento dei dati, inizialmente raccolti per finalità di diagnosi e cura, ad un ulteriore trattamento connesso a finalità di ricerca scientifica.
8.	**Quali procedure vengono adottate per verificare che**	Il protocollo condiviso e autorizzato con il Comitato

	le modalità di raccolta dei dati sono adeguate, coerenti e non eccessive, in relazione alle finalità per i quali i dati vengono trattati?	Etico stabilisce sia il set di informazioni cui si può accedere, sia il dataset di informazioni che devono essere poi successivamente raccolte, catalogate e valutate, oltre che all'arco temporale di analisi.
9.	**Con quali modalità viene verificata la accuratezza dei dati personali raccolti e trattati?**	L'accuratezza dei dati personali raccolti viene garantita mediante gli identificatori utilizzati per l'estrazione.
10.	**È stata effettuata una valutazione circa il fatto che il trattamento dei dati personali raccolti potrebbe causare danni ai diritti e alle libertà agli interessati coinvolti?**	Sì
11.	**È stato stabilito un periodo massimo di conservazione dei dati?**	Sì, 10 anni dal termine dello studio.
12.	**Quali misure tecniche e organizzative di sicurezza sono state adottate per prevenire qualsivoglia trattamento di dati personali non autorizzato o illegittimo?**	Si rimanda al punto 7.5 e all'appendice B
13.	**È previsto il trasferimento di dati personali in un paese non facente parte dell'unione europea?** **Se sì, quali provvedimenti sono stati adottati per garantire che i dati siano salvaguardati in modo appropriato?**	N/A

Appendice B - Tabella dei rischi afferenti alla DPIA

Descrizione del rischio	Rischi inerenti alla protezione dei dati			Opzioni che permettono di evitare o mitigare questo rischio [31]	Rischi residui		
	Impatto	Probabilità	Rischio	(opzioni/controlli applicati)	Impatto	Probabilità	Rischio
Distruzione	**2**	**2**	**BASSO**	• Gli applicativi aziendali garantiscono protezione nei confronti di eventi che potrebbero comportare la distruzione del dato per via della ridondanza e backup delle informazioni e la possibilità di effettuare nuove estrazioni in caso di distruzione accidentale dei dati. • Il monitoraggio dell'infrastruttura è in grado di rilevare e segnalare le possibili anomalie, per assicurare il corretto funzionamento dei servizi aziendali.	**1**	**2**	**BASSO**
Perdita	**2**	**1**	**BASSO**	• Possibilità di effettuare nuove estrazioni in caso di perdita accidentale dei dati partendo dai dati clinici iniziali (questi sono conservati in database protetti da misure di sicurezza gestiti a livello centralizzato). • Sono implementate tecniche di pseudonimizzazione tali da non consentire a chi eventualmente entri in possesso dei dati, anche a seguito di smarrimento, di poter re identificare i soggetti interessati senza l'utilizzo di informazioni aggiuntive.	**1**	**1**	**BASSO**
Distribuzione non	**3**	**3**	**MEDIO**	• Anonimizzazione dataset per svolgimento dell'analisi statistica e	**2**	**2**	**BASSO**

[31] nota: per ogni rischio afferente alla protezione dei dati, possono essere disponibili varie opzioni che permettono di evitare o mitigare questo rischio. È appropriato elencare tutte le opzioni disponibili e quindi valutare il rischio residuo, in conseguenza dell'applicazione di ogni specifica opzione. Fare riferimento alla normativa europea EN 31000

autorizzata				pubblicazione dei risultati esclusivamente in forma anonima e aggregata.			
Accesso ai dati non autorizzato	**3**	**3**	**MEDIO**	• L'accesso ai sistemi contenenti dati personali (PC, cartelle condivise, database etc.) avviene tramite codice ID e password, attribuiti a ciascun utente univocamente e individualmente. • Gli strumenti di autenticazione (password) sono comunicate agli utenti in modo tale che sia mantenuta la loro riservatezza e non vengono comunicate o usate da altri utenti. • Le password sono cambiate periodicamente, è richiesta una lunghezza minima (almeno otto caratteri oppure un numero di caratteri pari al massimo consentito dal sistema) e devono contenere almeno due tipologie diverse di caratteri (ad es. lettere, numeri, caratteri speciali, maiuscoli etc.) • Esistono autorizzazioni specifiche per diversi utenti o categorie di utenti, limitando l'accesso ai soli dati strettamente necessari per l'espletamento delle attività. Sono limitati e controllati l'assegnazione e l'uso di diritti di accesso privilegiato. • Esiste un processo strutturato e formalizzato che prevede la creazione, modifica e cancellazione degli utenti in caso di inizio, cambio o cessazione del rapporto di lavoro o delle mansioni. • Periodicamente avviene la rivisitazione dei diritti di accesso degli utenti e viene verificato periodicamente l'effettivo allineamento tra ID/account attivi e utenti autorizzati.	**2**	**2**	**BASSO**

				• Sono previsti inoltre sistemi antintrusione e procedure per controllare l'accesso fisico ai locali			
Trattamento non autorizzato	**2**	**4**	**MEDIO**	• Predeterminazione nell'ambito del protocollo di studio del novero dei dati clinici oggetto di accesso: il soggetto che è autorizzato ad analizzare i dati di partenza andrà a selezionare e trattare solamente dati già preventivamente concordati; • Controllo degli accessi logici; • Gestione postazioni; Controllo degli accessi fisici.	**2**	**2**	**BASSO**
Trattamento non conforme alla finalità della raccolta o illecito	**2**	**2**	**BASSO**	• Istruzioni specifiche ai soggetti autorizzati: i dati raccolti seguono un protocollo di ricerca che ne definisce gli obiettivi e il disegno, conseguentemente definisce i limiti e gli ambiti di trattamento dei dati; • A livello Aziendale: -gestione, formazione e sensibilizzazione del personale; -adozione di politiche e procedure di sicurezza.	**2**	**1**	**BASSO**

Legenda

Probabilità (P)		
1	molto bassa	accade solo in circostanze eccezionali (P < 5%)
2	bassa	è improbabile che accada (5% < P < 20%)
3	media	può accadere in un certo numero di casi (20% < P < 50%)
4	alta	avviene in una buona parte dei casi (50% < P < 75%)
5	molto alta	avviene nella maggior parte dei casi (P > 75%)

Impatto o Entità del Danno (I)		
1	molto bassa	insignificante
2	bassa	Bassa
3	media	Moderata
4	alta	Elevate
5	molto alta	Catastrofica

	Probabilità (P)

Impatto(I)	molto bassa (1)	bassa (2)	media (3)	alta (4)	molto alta (5)
molto bassa (1)	1	2	3	4	5
bassa (2)	2	4	6	8	10
media (3)	3	6	9	12	15
alta (4)	4	8	12	16	20
molto alta (5)	5	10	15	20	25

area	livelli	entità di rischio
B	1 - 4 (rischio accettabile)	bassa (B)
M	5 - 14 (rischio da ridurre)	media (M)
A	15 - 25 (rischio da ridurre immediatamente)	alta (A)