

ESTRATTO VALUTAZIONE DI IMPATTO STUDIO TRRD

1. Informazioni generali

1.1 Titolare del trattamento

La presente DPIA è stata redatta dall'ASST dei Sette Laghi, in qualità di Titolare del trattamento ("Titolare del trattamento" o "ASST").

Tale ruolo è assunto in quanto l'ASST ha determinato finalità e mezzi di trattamento.

Il Responsabile del progetto è la dott.ssa Francesca Ilaria Cortellaro

1.2 Contesto di riferimento

Oggetto della presente valutazione d'impatto (Data Protection Impact Assessment – DPIA) è il trattamento dei dati personali dei pazienti relativo allo studio **"Efficacia e sicurezza della gestione domiciliare dei pazienti fragili dimessi dal pronto soccorso e gestiti dal team di risposta rapida domiciliare (TRRD)"**

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;
- 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 [prov. GPDP 497/2018 riguardante le aut. gen. 9/2016 e aut. gen. 8/2016];
- 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 Techniques, 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 il 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 personali relativi ai pazienti arruolati nell'ambito del progetto 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);
- Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento – (rif. 12).

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.

2.2 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.

3. Fase 1: Descrizione del trattamento

3.1.1 Il trattamento oggetto della Valutazione di Impatto

Il Team di Risposta Rapida Domiciliare è un servizio di transitional care tra medicina ospedaliera e medicina territoriale, attraverso il quale si prendono in carico pazienti fragili dimessi dal Pronto Soccorso dell'Ospedale di Circolo di Varese (ASST Sette Laghi, Lombardia) in condizioni cliniche generali stabili e che hanno concluso tutti gli accertamenti necessari in regime di urgenza ma necessitano, entro le 24 ore successive, di un ulteriore periodo di osservazione per rivalutazione clinica, controllo di esami ematici, elettrocardiogramma o ecografia clinica focalizzata (ecografia point of care) e prosecuzione di terapia medica per un periodo che oscilla tra i 3 e i 5 giorni successivi. Lo scopo del lavoro è volto a valutare la sicurezza e l'efficacia della gestione domiciliare dei pazienti fragili.

I risultati ottenuti nella popolazione trattata a domicilio verranno confrontati con quelli relativi a pazienti fragili ricoverati, potenzialmente arruolabili per caratteristiche cliniche al trattamento domiciliare con TRRD, ma esclusi per criteri territoriali, mancanza di setting assistenziale e/o caregiver adeguati.

La sicurezza verrà valutata confrontando il tasso di complicanze e/o di mortalità tra i due gruppi.

L'efficacia verrà valutata in relazione al numero di rientri entro 10 giorni dalla dimissione con TRRD o dalla dimissione ospedaliera.

Questo studio prevederà un modello osservazionale prospettico e retrospettivo monocentrico. Per la parte retrospettiva dello studio verranno inclusi i pazienti fragili che hanno soddisfano i criteri di inclusione e che sono stati gestiti con TRRD o ricoverati in reparto a partire dal 18 dicembre 2024. Per l'analisi prospettica verranno inclusi i pazienti con gli stessi criteri di inclusione e che avranno aderito allo studio previa acquisizione del Consenso Informato. Per quei pazienti i cui dati sono raccolti retrospettivamente e per i quali non fosse possibile l'ottenimento del Consenso Informato, si procederà al trattamento dei dati personali in ottemperanza alle normative vigenti. (ved. Dichiarazione_sostitutiva_di_modulo_consenso)

Verranno arruolati consecutivamente pazienti fragili, le cui caratteristiche verranno riportate in seguito, che accedono al Pronto Soccorso dell'Ospedale di Circolo e Fondazione Macchi di Varese per una problematica acuta o acuta su cronica con indicazione a prosecuzione di monitoraggio clinico e terapia, controllo di esami ematici e approfondimento o monitoraggio con ecografia clinica focalizzata.

Questi pazienti in Pronto Soccorso vengono preferibilmente assegnati ad un'area dedicata ai pazienti fragili e quindi arruolati al trattamento con TRRD dal personale medico di PS.

In particolare le principali problematiche cliniche oggetto di arruolamento saranno:

Scompenso cardiaco, BPCO riacutizzata, polmoniti, infezioni vie urinarie complicate, disidratazione, alterazioni elettrolitiche, anemia sideropenica in perdita GE acuta su cronica, gestione del dolore acuto non controllato, traumi toracici lievi, tachiaritmie in rate control.

Il medico di PS, dopo aver illustrato l'informativa al paziente e/o al caregiver e aver ottenuto consenso informato firmato da parte del paziente o del tutore legale, attiva il servizio TRRD. La presa in carico a domicilio deve avvenire entro le 24 ore successive, tramite visita domiciliare e/o televisita.

La raccolta dei dati verrà eseguita tramite consultazione di cartelle cliniche, referti di laboratorio, referti microbiologici presenti sui sistemi informatici in dotazione ad ASST SETTE LAGHI ed AREU.

Modalità di consegna dell'informativa:

Il medico di PS, illustra l'informativa privacy al paziente e/o al caregiver e ottiene il consenso firmato da parte del paziente o del tutore legale.

- Data di inizio prevista: 18/12/2024
- Durata stimata del progetto: 30/04/2026

L'obiettivo dello studio è quello di valutare la sicurezza e l'efficacia della gestione domiciliare del TRRD in pazienti fragili dimessi dal Pronto Soccorso dell'Ospedale di Circolo di Varese (ASST Sette Laghi, Lombardia).

In particolare, la sicurezza del servizio, che rappresenta la possibilità di ricevere a domicilio le medesime cure che il paziente avrebbe ricevuto se sarà stato ospedalizzato, verrà valutata considerando complicanze e mortalità del gruppo trattati con TRRD, confrontate con il gruppo di pazienti non trattati ma ricoverati.

L'efficacia invece si misurerà valutando la percentuale di rientri in PS entro 10 giorni tra il gruppo di pazienti trattati al domicilio con il TRRD e quello di pazienti ospedalizzati; rientri che dovranno essere sempre per la stessa problematica oggetto dell'attivazione del TRRD o dell'ospedalizzazione.

Potenziali benefici derivanti dal progetto:

Valutare sicurezza ed efficacia della gestione domiciliare del paziente Fragile in alternativa al ricovero ospedaliero, riducendo i rischi connessi a tale trattamento. Contestuale riduzione del Boarding ed ottimizzazione delle risorse ospedaliere. Ottimizzare la rete ospedale territorio.

Potenziali rischi derivanti dal progetto:

Non sono stati identificati rischi connessi al progetto

3.1.2 Ruoli e responsabilità collegate al trattamento.

I soggetti che possono intervenire oltre il Titolare del trattamento sono eventuali fornitori nominati come Responsabili del trattamento secondo l'ex art. 28 del GDPR.

Per lo Studio in questione non risultano essere stati nominati Responsabili del trattamento.

In ogni caso il personale che accede ad archivi contenenti dati personali anche solo indirettamente identificativi è stato autorizzato se subordinato/parasubordinato (ai sensi dell'art. 29 GDPR) oppure nominato Responsabile ex art. 28 GDPR negli altri casi.

Il PI e personale sanitario o tecnico autorizzato dall'ASST Sette Laghi e formalmente formato per la gestione dei dati personali.

3.1.2.1.1 Persone fisiche che intervengono nel trattamento

Nel trattamento intervengono:

- **Il Responsabile del progetto:** Dott.ssa Francesca Ilaria Cortellaro
- Personale sanitario in servizio presso S.C. PRONTO SOCCORSO E MEDICINA D'URGENZA OSPEDALE CIRCOLO E FONDAZIONE MACCHI VARESE ASST SETTE LAGHI

3.2 Dati, processi e beni di supporto

3.2.1 Dati trattati

I dati personali relativi ai pazienti arruolati sono definiti nel documento “CRF Studio 96_2025” (cfr. Allegato 1).

Dati personali del paziente:

- Dati anagrafici: nome, cognome, età, sesso;
- Dati di contatto: residenza, indirizzo mail, telefono;
- Dati relativi alla salute

Per l'adozione delle necessarie misure di sicurezza si trattano i seguenti dati degli operatori sanitari.

- Credenziali di accesso
- Fattore di autenticazione (password, ID token)
- Mail aziendali

3.2.2 Fonti dei dati

I dati dei pazienti utilizzati per le finalità del progetto sono acquisiti dai soggetti autorizzati dall'ASST tramite i sistemi informativi ospedalieri e tramite la raccolta manuale, registrati e organizzati in fogli Excel pseudonimizzati, su PC aziendale, accessibile solo al personale autorizzato.

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.

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:
 - Software aziendali di gestione pazienti in Pronto Soccorso (NGH) e Reparti (W Hospital, Portale di Reparto), TRRD (applicativo AREU CMU)
- Sistema per la gestione del Data Collection Template:
 - Fogli di calcolo Excel

Infrastruttura:

- Share di rete su Cloud Microsoft (One Drive) dove sarà creata una cartella specifica per questo studio dall'owner: Dott.ssa Francesca Ilaria Cortellaro. Lo spazio One Drive che contiene questa cartella verrà sottoposto a backup tramite una piattaforma OnPrem. L'accesso a questa cartella avviene solo con credenziali personali e in caso di accesso esterno viene imposto un secondo fattore di autenticazione. Questa cartella conterrà il file excel strutturato per la gestione dei dati pseudonimizzati. Questo documento verrà condiviso con il personale interno. In caso di dimissioni dell'owner il file andrà trasferito. E' responsabilità dell'owner gestire la condivisione del documento.
- Share di rete su server aziendale ubicata presso la sala server dei Sistemi Informativi. Tale cartella viene sottoposta a backup locale su NAS secondaria e su Cloud tramite piattaforma Rubrik. Questa cartella conterrà un file excel contenente le informazioni chiave per poter risalire all'anagrafica in caso di necessità. L'accesso a questa cartella sarà possibile solo al Dott.... attraverso le proprie credenziali personali e non avrà possibilità di delega che, in caso di necessità, potrà essere inserita o modificata solo dai Sistemi Informativi Aziendali.

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 contrapporre 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 cura e la sicurezza del paziente. Queste richiedono una collegabilità del dato 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: valutare la sicurezza e l'efficacia clinica del TRRD confrontando i dati raccolti con una popolazione di pazienti sottoposti a ricovero convenzionale

Esse vengono esplicitate nell'informativa privacy Versione 1.2 del 09/01/2026 (cfr. Allegato 2).

4.1.2 Fondamenti legali del trattamento

La base giuridica del trattamento si fonda su:

Per la parte retrospettiva:

- Consenso (art. 6, par. 1, lett. a, GDPR e art. 9, par. 2, lett. a, GDPR) laddove l'interessato possa essere ricontattato;
- Pubblico interesse ai fini del trattamento per finalità di ricerca scientifica ex Art. 9, par. 2, lett. j) del GDPR e applicazione dell'Art. 110 del Cod. privacy (D.lgs. 30 giugno 2003, n. 196) laddove “*a causa di particolari ragioni, 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*” (v. Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice - 9 maggio 2024 [10016146] e Allegato 2 “Dichiarazione sostitutiva di modulo di consenso informato e consenso al trattamento dei dati personali”).

Per la parte prospettica:

- Consenso dell'interessato ex art. 6, par.1 lett. a) e art. 9, par. 2, lett. a) GDPR.

Il consenso è:

- a. liberamente conferito: la scelta di partecipare allo studio è opzionale e facoltativa, in quanto non l'interessato non subisce conseguenze negative in termini di assistenza sanitaria ricevuta.
- b. specifico: il consenso viene richiesto per ogni specifica finalità che lo prevede.
- c. informato: all'interessato sono fornite le opportune informazioni ai sensi degli artt. 12-13 del GDPR.
- d. inequivocabile: il consenso viene prestato attraverso l'apposizione di firma quale azione positiva dell'utente

- e. esplicito: la richiesta di consenso è costruita in modo tale da presentare all'utente sia l'opzione di acconsentire sia l'opzione di non acconsentire al trattamento
- f. revocabile in qualsiasi momento: l'interessato può esercitare il diritto di revoca tramite richiesta effettuata al Titolare del trattamento nella persona del Responsabile dello studio

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.

4.1.4 Accuratezza ed aggiornamento dei dati

Si fa riferimento alla correttezza dei dati raccolti e riportati nella cartella clinica del paziente partecipante. I dati sono raccolti e trattati da un numero ristretto di persone: i sanitari che hanno in cura il paziente.

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 nel progetto, come descritto nel paragrafo **Error! Reference source not found.** La chiave per risalire all'oggetto sarà conosciuta solo dalla PI e dal personale sanitario che ha partecipato allo studio.

I dati raccolti saranno oggetto di un'attività di anonimizzazione, sulla base del WP 216 5/2014 per la pubblicazione e alla fine del progetto.

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 tabella di correlazione contenenti i dati anagrafici e direttamente identificativi del paziente saranno conservati in modalità segregata per 7 anni dopo il termine del progetto.

I risultati del progetto (dati anonimi) verranno conservati a tempo indeterminato.

I dati di autorizzazione, identificazione ed accesso ai sistemi sono conservati per un 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. Come indicato nel Protocollo di studio il medico di PS, dopo aver illustrato l'informativa al paziente e/o al caregiver e aver ottenuto consenso

informato firmato da parte del paziente o del tutore legale, attiva il servizio TRRD. La presa in carico a domicilio deve avvenire entro le 24 ore successive, tramite visita domiciliare e/o televisita.

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 progetto, ai sensi dell'art. 17 del GDPR.

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 Obblighi dei responsabili del trattamento

Non sono presenti responsabili del trattamento.

4.3 Trasferimenti al di fuori dello SEE

Non vengono effettuati trasferimenti al di fuori dello Spazio Economico Europeo come indicato anche nell'Informativa privacy consegnata al paziente

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 artt. 13 e 14 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 6: Calcolo del rischio residuo, piano di remediation e parere del DPO

5.1 Rischio residuo

Si ritiene che il rischio residuo collegato al trattamento di dati personali per le finalità del progetto 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.

5.2 Piano di remediation

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

5.3 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 "Studio n. 96 - 2025", nello svolgimento dei compiti attribuitigli, ha valutato che:

L'indice del documento e i 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*). La metodologia di calcolo del livello del rischio è conforme all'approccio metodologico ENISA (Agenzia dell'Unione europea per la cibersicurezza).

In rapporto alle finalità e alla tipologia di dati trattati, le misure di sicurezza applicate, specialmente il rispetto di quelle cautele dettate dal Garante con le Prescrizioni sui dati genetici e le Prescrizioni e le Regole Deontologiche in materia di ricerca scientifica, appaiono adeguate a rispettare i dettami dell'art. 32 del GDPR nonché, più in generale, i diritti e le libertà fondamentali degli individui.

Il DPO si riserva, comunque, successive e più approfondite valutazioni anche a seguito dei possibili riscontri che potrebbero pervenire dagli interessati, ovvero in caso di acquisizione di ulteriori, diverse e rilevanti informazioni. In quest'ottica, qualora la concreta applicazione del trattamento lo richiedesse, dovranno essere implementate eventuali misure correttive che, nel caso, condurranno altresì ad un aggiornamento della presente DPIA.

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

Dato che il trattamento dei dati personali non rientra nei casi previsti, il Titolare non procederà alla consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR.

