

ESTRATTO VALUTAZIONE DI IMPATTO STUDIO PROTOCOLLO AI DERM

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 il dott. Andrea Carugno

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 **"Riconoscimento e localizzazione di lesioni cutanee ad alto rischio da immagini dermatologiche mediante tecniche di Intelligenza Artificiale"**

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;
- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Legge sull'intelligenza artificiale);
- ISO/IEC 42001:2023 - Sistema di Gestione IA

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 effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 – (rif. 7);
- 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.

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 presente studio si propone di sviluppare e validare un modello di deep learning per l'analisi di immagini cliniche e dermoscopiche di lesioni cutanee ad alto rischio, con i seguenti obiettivi specifici:

1. Individuazione e localizzazione delle lesioni cutanee sospette
 - a. Sviluppare un modello in grado di identificare e localizzare le lesioni a rischio (melanomi, carcinomi cutanei e altre lesioni potenzialmente maligne) attraverso l'uso di bounding box per evidenziare le aree di interesse.
2. Classificazione delle lesioni cutanee
 - a. Classificazione binaria: distinguere tra lesioni benigne e maligne, a supporto della stratificazione del rischio clinico.
 - b. Classificazione multiclasse: riconoscere e categorizzare le principali tipologie di lesioni cutanee (melanomi, nevi, carcinomi basocellulari, carcinomi squamocellulari, cheratosi seborroiche, ecc.), al fine di aumentare la specificità del modello.
3. Valutazione delle prestazioni del modello
 - Analizzare le performance in termini di:
 - Precisione (riduzione dei falsi positivi)
 - Recall (identificazione di tutte le lesioni sospette)
 - mAP (Mean Average Precision) per l'accuratezza del rilevamento delle lesioni.
 - Calcolare le metriche chiave per la classificazione, tra cui:
 - Accuratezza
 - AUROC (Area Under the Receiver Operating Characteristic Curve)
 - Matrici di confusione per l'analisi degli errori di classificazione.
4. Valutazione dell'impatto clinico potenziale del modello
 - Stimare, su base teorica, la capacità del modello di ridurre il numero di escissioni chirurgiche non necessarie e di ottimizzare l'uso delle risorse diagnostiche e terapeutiche.
5. Confronto tra architetture di deep learning
 - Indagare l'applicabilità e le prestazioni di modelli basati su architetture di nuova generazione, in particolare Transformer (es. Deformable DETR, Swin Transformer), confrontandoli con modelli consolidati (es. YOLOv7), per identificare la soluzione più accurata e affidabile nell'analisi delle immagini dermatologiche.

Modalità di raccolta dei dati

Il dataset sarà costituito da immagini cliniche e dermoscopiche di lesioni cutanee, archiviate presso la SC Dermatologia dell'ASST Sette Laghi. Per i pazienti tuttora afferenti a follow-up clinici presso la struttura, l'utilizzo delle immagini sarà subordinato alla raccolta di consenso informato scritto, che autorizza l'uso retrospettivo dei dati già archiviati.

Per i pazienti non più seguiti o deceduti, verranno utilizzate esclusivamente immagini già anonimizzate, non più riconducibili all'identità individuale.

Caratteristiche del dataset

- Tipologie di lesioni incluse: melanomi, nevi melanocitici, cheratosi seborroiche, carcinomi basocellulari, carcinomi squamocellulari e altre lesioni cutanee di interesse diagnostico.
- Numero di immagini: l'obiettivo è raggiungere un dataset composto da migliaia di immagini, in grado di fornire una base solida per l'addestramento e la validazione dei modelli. Sarà

garantito un adeguato bilanciamento tra lesioni ad alto e basso rischio, al fine di ridurre bias nelle prestazioni.

Modalità di consegna dell'informativa:

Lo studio, pur essendo retrospettivo, prevede la raccolta del consenso informato dai pazienti che accedono tuttora ai controlli clinici, al fine di autorizzare l'uso delle immagini archiviate in passato. La partecipazione è volontaria e l'eventuale rifiuto non comporterà alcuna conseguenza sul percorso assistenziale.

- Data di inizio prevista: 01/04/2026
- Durata stimata del progetto: 12 mesi complessivi, inclusivi di raccolta dati retrospettiva, anonimizzazione, addestramento modelli, analisi e redazione dei risultati.

Gli obiettivi dello studio sono:

- Individuazione e localizzazione delle lesioni cutanee sospette;
- Classificazione delle lesioni cutanee;
- Valutazione delle prestazioni del modello;
- Valutazione dell'impatto clinico potenziale del modello;
- Confronto tra architetture di deep learning;

L'obiettivo finale è migliorare il percorso di gestione delle lesioni cutanee sospette attraverso:

- un triage più accurato delle lesioni dubbie da parte del medico di medicina generale, con rapida identificazione dei pazienti che necessitano di valutazione specialistica prioritaria;
- la riduzione dei tempi di attesa per la visita dermatologica, grazie a un primo screening automatizzato più efficiente;
- l'incremento dell'accuratezza diagnostica complessiva, mediante l'integrazione dell'intelligenza artificiale con la dermoscopia per supportare il processo decisionale clinico;
- la limitazione delle escissioni chirurgiche non necessarie, favorendo un approccio diagnostico-terapeutico più mirato e riducendo l'impatto psicologico ed economico sul paziente e sul sistema sanitario.

Potenziali benefici derivanti dal progetto:

Il progetto mira a generare un significativo miglioramento dell'outcome clinico attraverso l'incremento dell'accuratezza diagnostica, permettendo l'identificazione tempestiva delle lesioni maligne e migliorando conseguentemente la prognosi dei pazienti. L'aumento della specificità del modello consentirà inoltre di ridurre il numero di escissioni chirurgiche non necessarie, limitando l'impatto fisico e psicologico sui soggetti coinvolti. A livello di sistema sanitario, l'introduzione di questo strumento di supporto decisionale potrà favorire un triage più efficiente da parte della medicina generale, ottimizzando le liste d'attesa specialistiche e l'allocazione delle risorse, oltre a contribuire all'avanzamento scientifico validando l'efficacia delle più recenti architetture di Deep Learning in ambito dermatologico.

Potenziali rischi derivanti dal progetto:

I rischi associati allo studio sono limitati e riguardano principalmente la possibilità di bias algoritmici, ovvero l'eventualità che il modello possa presentare performance non uniformi su sottogruppi di

lesioni meno rappresentate nel dataset; tale criticità viene tuttavia mitigata attivamente attraverso strategie di bilanciamento dei dati tra classi ad alto e basso rischio. Relativamente alla privacy e alla sicurezza delle informazioni, i potenziali rischi sono efficacemente mitigati dall'adozione di rigorose tecniche di anonimizzazione, protezione e conservazione dei dati, come dettagliatamente illustrato nella sezione successiva del documento.

3.1.2 Ruoli e responsabilità collegate al trattamento.

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

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.

3.1.2.1.1 Persone fisiche che intervengono nel trattamento

Nel trattamento intervengono:

- **Il Responsabile del progetto:** assume il ruolo di designato/delegato, cioè di autorizzato con ruolo di impostazione e coordinamento
- **Data manager:** non previsto
- **Statistico:** non previsto

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 140_2025” (cfr. Allegato 1).

Dati personali del paziente:

- Dati anagrafici essenziali (età, sesso, fototipo);
- Dati relativi alla salute (immagini cliniche e dermoscopiche di lesioni cutanee, diagnosi cliniche e istopatologiche correlate, se disponibili);
- Eventuali metadati clinici anonimizzati (localizzazione anatomica, data acquisizione immagine).

Tutti i dati saranno anonimizzati o pseudonimizzati tramite codici numerici.

Non è previsto il trattamento dei dati degli operatori sanitari (Non sono previsti LOG accessi. Sistemi offline.)

3.2.2 Fonti dei dati

I dati dei pazienti utilizzati per le finalità del progetto sono le immagini e i metadati acquistati dall'archivio del videodermatoscopio Fotofinder Vexia presente presso la SC Dermatologia. In caso di disponibilità, verranno correlate con l'esame istologico relativo alle lesioni osservate.

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: Non è previsto alcun trasferimento a soggetti terzi o industrie farmaceutiche.

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:
 - Foto cliniche con metadati
 - Esame istologico
- Sistema per la gestione del Data Collection Template:
 - Non verranno usati sistemi di archiviazione dei dati, l'analisi verrà effettuata esclusivamente sulle immagini con eventuali metadati e i risultati non saranno archiviati in documenti/DB con Funzione di Data Collection.

Infrastruttura:

- Strumento Fotofinder Vexia in qualità di sorgente delle informazioni da analizzare (immagini e metadati)

Lo strumento non è connesso alla rete e non ne è prevista la connessione.

- Disco esterno usato per il travaso dei dati dallo strumento al Computer destinato all'elaborazione.

Questo disco dovrà essere sottoposto a verifica di sicurezza e formattazione prima dell'uso, e a cancellazione sicura al termine dell'uso che viene identificato con il termine della copia dei dati sul Computer di elaborazione. I Sistemi informativi Aziendali daranno supporto.

- Computer dedicato all'elaborazione, isolato dalla rete e fisicamente localizzato presso stanza direttore della SC Dermatologia, piano 3, padiglione 6, ASST dei Sette Laghi.

Il Computer è di fornitura esterna (Università Uninsubria). Il fornitore si occuperà di garantire un sistema aggiornato e protetto anche se verrà mantenuto Off Line. Allo stesso modo il fornitore dovrà consegnare al responsabile di questo studio delle credenziali con i livelli minimi di privilegi necessari.

Su questo computer verranno caricati i dati da elaborare e verrà eseguita una prima elaborazione per l'anonimizzazione.

Al termine dell'elaborazione clinica, questo computer rimarrà conservato presso l'armadio chiuso a chiave della stanza del direttore della SC Dermatologia, piano 3, padiglione 6, ASST dei Sette Laghi, sotto la supervisione di Andrea Carugno per un periodo di 12 mesi.

Allo scadere del periodo conservazione, il computer dovrà essere sottoposto a cancellazione sicura del disco prima del riutilizzo e/o comunque prima del trasferimento fisico ad altre sedi.

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:

- Finalità di ricerca

Esse vengono esplicitate nell'informativa (cfr. Allegato 1).

4.1.2 Fondamenti legali del trattamento

La base giuridica del trattamento si fonda su:

- Per la parte retrospettiva: art. 6, par. 1, lett. e) e art. 9, par. 2, lett. j) GDPR; art. 110 del d.lgs. n. 196/2003 (Codice privacy) laddove risulta impossibile o implicherebbe uno sforzo sproporzionato acquisire il consenso del paziente
- 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 moda 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 dallo sperimentatore principale.

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).

I dati raccolti saranno conservati per 10 anni dalla conclusione dello studio, in conformità alle disposizioni normative e alle linee guida nazionali e regionali.

I dati di autorizzazione, identificazione ed accesso ai sistemi sono conservati per 10 anni.

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 care giver 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 stati individuati responsabili del trattamento ex art. 28 GDPR.

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. 140 del 2025 - Riconoscimento e localizzazione di lesioni cutanee ad alto rischio da immagini dermatologiche mediante tecniche di Intelligenza Artificiale", 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.