VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) PER LE ATTIVITÀ DI RICERCA CLINICA NELLO STUDIO RETROSPETTIVO

"Valutazione della capacità predittiva di alcuni indici antropometrici nell'identificare la sindrome metabolica in bambini e adolescenti obesi affetti da sindrome di Prader-Willi (PWSOBIPMETS)"

Abstract

Il presente documento rappresenta una Valutazione di Impatto richiesta ai sensi degli artt. 35 e 36 del Regolamento UE 2016/679 e degli artt. 110 e 110bis del D.lgs. 193/2003. L'Istituto Auxologico italiano effettua uno studio multicentrico di ricerca (progetto PWS-FOLLOWUP) a partire dai dati raccolti durante la pratica clinica di pazienti che si sono sottoposti ai servizi sanitari dell'Istituto Auxologico Italiano. I dati vengono trattati dal personale per l'effettuazione dello studio retrospettivo dal titolo "Valutazione della capacità predittiva di alcuni indici antropometrici nell'identificare la sindrome metabolica in bambini e adolescenti obesi affetti da sindrome di Prader-Willi"

Redatto	Verificato		Approvato
DPO Dott. Valerio Gatti	Medici Referenti Dott. Graziano Grugni; Dott. Alessandro Sartorio		Dott. Mario Colombo

SOMMARIO

DEFINIZIONI E ABBREVIAZIONI

DPIA	Valutazione d'impatto (*Data Protection Impact Assessment*) - Valutazione ai sensi dell'art. 35 del GDPR che il Titolare del trattamento dei dati è chiamato a svolgere in via preliminare ogni volta che si appresta ad eseguire un trattamento che, per la natura, lo scopo o l'ambito di applicazione potrebbe presentare un elevato rischio specifico per i diritti e le libertà dell'interessato.
GDPR	Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). È il principale testo normativo europeo in materia di protezione dei dati personali.
Codice Privacy	Decreto Legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".
Anonimizzazione	È una operazione di trattamento che attraverso la de-identificazione trasforma in maniera irreversibile i dati personali in dati anonimi in modo tale che non si possano più attribuire a un interessato specifico.
Pseudonimizzazione	Il trattamento dei dati in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile
PI/Sperimentatore	*Principal Investigator*, Ricercatore responsabile dell'esecuzione dello studio. Se lo Studio è svolto da un gruppo di persone nello stesso centro, lo sperimentatore responsabile del gruppo è definito Sperimentatore principale.
Garante Privacy	Trattasi del Garante per la protezione dei dati personali, autorità amministrativa indipendente istituita dalla legge sulla privacy (legge 31 dicembre 1996 n. 675). Il Garante privacy è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (GDPR).
Titolare	Trattasi della persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Responsabile	Persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del Titolare

	del trattamento dei dati personali e in base alle sue istruzioni.

1. Perché questa DPIA

a. *Premessa*

La Fondazione Istituto Auxologico Italiano (di seguito, **"Istituto Auxologico"** o anche **"Titolare"**), riconosciuta come Istituto di Ricovero e Cura a Carattere Scientifico (IRCCS) ai sensi del d.lgs. 288/2003, dal 1972, è un istituto di eccellenza dedicato alla cura medica delle persone. Oltre alla sua missione clinica, Istituto Auxologico si distingue per il suo impegno nella ricerca scientifica e clinica, promuovendo e realizzando progetti con l'obiettivo di migliorare in modo sistematico e costante l'offerta terapeutica.

La ricerca clinica, parte integrante e centrale delle attività di Istituto Auxologico, mira a determinare, su soggetti umani, la sicurezza e l'efficacia di ogni approccio clinico, inclusi dispositivi, prodotti diagnostici, farmaci o soluzioni innovative, comprese combinazioni di questi. Tale ricerca abbraccia pratiche preventive, diagnostiche e terapeutiche, strettamente collegate allo sviluppo e all'ottimizzazione della stessa, nel pieno rispetto delle Good *Clinical Practices* (GCP) e degli *standard*, delle norme, delle linee guida, nazionali ed internazionali, vigenti per la ricerca clinica, sia su farmaco che su dispositivo.

L'attività di ricerca clinica di Istituto Auxologico si esplica, nel caso di specie, nella tipologia di ricerca osservazionale retrospettiva, ossia uno studio clinico che non ha impatti diretti sulla terapia del paziente, ma è basato solo su raccolta retrospettiva e analisi di dati raccolti nell'ambito della terapia *standard* (in riferimento a quanto disposto dall'art. 2, paragrafo 2, n. 4 del Regolamento UE 536/2014).

Il *Principal Investigator*, il *co-principal investigator* e *i ricercatori afferenti al laboratorio di ricerca* effettuano uno studio retrospettivo osservazionale dal titolo "Valutazione della capacità predittiva di alcuni indici antropometrici nell'identificare la sindrome metabolica in bambini e adolescenti obesi affetti da sindrome di Prader-Willi (PWSOBIPMETS)". Lo scopo dello Studio, condotto in un gruppo di soggetti obesi affetti da PWS in età infanto-adolescenziale, è identificare l'indice caratterizzato dalla miglior prestazione classificatoria nella sindrome metabolica (MetS) e di confrontare tali risultati con quelli ottenuti in un gruppo di controllo con obesità semplice, al fine di verificare se le diverse peculiarità cliniche presenti nei due gruppi siano in grado di determinare eventuali differenze.

Lo studio è monocentrico e si basa su dati già raccolti durante la normale pratica clinica presso l'U.O. di Auxologia della sede di Istituto Auxologico in Piancavallo.

Lo Studio oggetto della presente DPIA è stato sottoposto all'autorizzazione del Comitato Etico competente, il quale ha rilasciato tale autorizzazione in data 17 marzo 2026.

Pertanto, lo scopo del presente documento è quello di fornire una valutazione d'impatto che il trattamento dei dati, relativo all'attività di ricerca, potrebbe avere sui diritti e sulle libertà dei soggetti interessati, al fine di valutarne la necessità e la proporzionalità.

b. *La normativa*

Secondo l'articolo 35 del Regolamento UE n. 2016/679 (di seguito **"GDPR"**) in presenza di un tipo di trattamento, che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento, prima di procedere al trattamento effettua una **Valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali** (di seguito **"DPIA"**).

In aggiunta, lo stesso articolo, prescrive lo svolgimento di DPIA in presenza di trattamenti quali, il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, par.1, come nel caso che riguarda lo Studio in oggetto che riguarda trattamenti di dati in grado di rivelare lo stato di salute di soggetti interessati. In generale, i trattamenti dei dati per finalità di ricerca rientrano nei casi previsti dal Garante Privacy (cfr. Allegato n.1 al Provvedimento del Garante n.467 dell'11 ottobre 2018 doc. web n. 9058979), in quanto trattasi di trattamenti non occasionali di dati relativi a soggetti vulnerabili, quali i pazienti.

Inoltre, come sarà indicato *infra* riguardo al ricorso dell'articolo 100 et 110bis del D.Lgs 193/2003 (di seguito **"Codice Privacy"**) come base giuridica su cui fondare le attività di trattamento relative ai dati personali per finalità di ricerca medica, biomedica ed epidemiologica, sono previste delle deroghe al principio stabilito dal GDPR che

prescrive il ricorso al consenso dell'interessato nel caso di trattamenti sui dati personali appartenenti alle categorie particolari, come i dati relativi alla salute degli interessati.

Per poter ricorrere a tali deroghe, come anche affermato nelle FAQ del Garante per la protezione dei dati personali, è necessaria la predisposizione e la pubblicazione di una DPIA.

c. *Gli studi retrospettivi*

Inoltre, il nuovo art. 110bis del Codice Privacy permette il trattamento ulteriore e secondario (c.d. **studi retrospettivi**) di dati personali relativi ai soggetti interessati raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico (**I.R.C.C.S.**), pubblici o privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del GDPR.

2. Chi è il titolare

Istituto Auxologico Italiano, con sede legale in via L. Ariosto n.13, Milano (MI), 20145 Italia è l'unico titolare al trattamento dei dati personali oggetto del presente Studio.

I dati di contatto sono i seguenti:

DPO Dott. Valerio Gatti

dpo@auxologico.it

PEC dpo.auxologico@pec.it

Ad avere accesso ai dati sono i soggetti preposti allo svolgimento dello Studio, soggetti nominati a persone autorizzate dal Titolare per il trattamento dei dati dei pazienti.

3. Una descrizione sistematica dei trattamenti

Il trattamento oggetto di valutazione riguarda la ricerca clinica, che incluse attività di natura osservazionale, concentrandosi dunque sulla raccolta e analisi dati senza intervenire direttamente sui soggetti arruolati.

All'interno del presente documento vengono analizzati i rischi connessi al trattamento dei dati personali dei soggetti interessati nell'ambito delle attività di ricerca clinica e verranno altresì illustrate le misure tecniche ed organizzative adottate dall'Istituto Auxologico per minimizzare tali rischi.

a. *Dati personali trattati*

Trattasi di dati raccolti durante la pratica clinica dei pazienti, tra i quali:

- Dati personali anagrafici (nome, cognome, sesso, età)
- Dati appartenenti a categorie particolari
- Dati in grado di rivelare lo stato di salute del soggetto, in particolare:
  - parametri antropometrici (altezza, peso, circonferenza vita)
  - parametri biochimici, comprendenti quelli basali legati alla diagnosi di MetS (colesterolo totale, HDL, trigliceridi, glicemia, insulinemia, HOMA-IR, emoglobina glicata, OGTT)
  - pressione arteriosa sisto-diastolica
  - rilievo anamnestico di terapia con anti-ipertensivi e/o antidiabetici e/o antilipemici.

Considerato l'utilizzo di sistemi informatici dell'Istituto Auxologico per l'estrazione e la pseudonimizzazione dei dati, possono inoltre essere trattati i dati di contatto del personale sanitario autorizzato, ove necessari per procedure interne, i log di accesso e tracciature informatiche generate dagli operatori abilitati, ai fini di sicurezza e audit.

b. *Categorie dei soggetti interessati*

La presente DPIA ha ad oggetto il trattamento dei dati personali dei pazienti minori, di età compresa tra 10 e 18 anni, affetti da Sindrome di Prader-Willi (PWS) e di soggetti con obesità essenziale, disponibili presso l'U.O. di Auxologia dell'IRCCS Istituto Auxologico Italiano (sede di Piancavallo), nonché del personale sanitario autorizzato (medici, ricercatori e personale tecnico) che accede ai sistemi informatici per l'estrazione, la pseudonimizzazione e l'analisi dei dati, generandone i relativi log di trattamento ai fini di sicurezza e audit.

c. *Le finalità*

Le finalità perseguite dallo Studio sono principalmente di ricerca clinica condotta sull'essere umano. L'attività di trattamento oggetto del presente DPIA è finalizzata al miglioramento delle cure, delle diagnosi e del trattamento clinico e di cura dei pazienti, anche tramite lo sviluppo di nuovi trattamenti o dispositivi medici.

d. *Le basi giuridiche*

Secondo il nuovo articolo 110, comma 1 del Codice Privacy il consenso dell'interessato per il trattamento dei dati personali relativi alla salute per fini di ricerca scientifica in campo medico, biomedico o epidemiologico non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, par. 2, lett. j) del GDPR, ossia il trattamento per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, incluso il caso in cui la ricerca in oggetto rientri in un programma di ricerca biomedica o sanitaria ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del GDPR.

Inoltre l'Istituto Auxologico, in quanto Istituto di Ricovero e Cura a Carattere Scientifico (IRCCS) privato, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta rispetto alla ricerca, ritiene e considera applicabile al trattamento di cui alla presente DPIA la deroga di cui all'art. 110 bis, comma 4, al divieto di trattare i dati relativi alla salute senza aver ottenuto il consenso dell'interessato (art. 9, comma 2, lett. a) del GDPR). Di conseguenza, è consentito l'utilizzo secondario per finalità di ricerca dei dati dei propri assistiti, raccolti per finalità di cura, in assenza del consenso.

Il trattamento e lo svolgimento dello Studio vengono effettuati in conformità anche dei seguenti *standard*:

- Dichiarazione di Helsinki;
- Convenzione di Oviedo "per la protezione dei Diritti dell'Uomo e della dignità dell'essere umano nei confronti dell'applicazione della biologia e della medicina: Convenzione sui Diritti dell'Uomo e la biomedicina" del 4 aprile 1997;
- Clinical Trials Regulation (Regolamento UE n.536/2014)
- Regole Deontologiche per trattamenti a fini statistici o di ricerca scientifica (Provvedimento del Garante Privacy del 19 dicembre 2018 n. 515);
- Provvedimento del Garante Privacy n.146 del 5 giugno 2019 recante le "Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del g.lgs. 10 agosto 2018, n.101";
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati, "GDPR").

e. *La durata di conservazione dei dati*

I dati utilizzati per lo Studio verranno conservati per una durata di 25 anni dalla raccolta dei dati personali.

f. Il ciclo di vita dei dati

L'attività di ricerca analizzata dal presente documento prende in esame i dati personali, compresi i dati appartenenti alle categorie particolari secondo il GDPR, raccolti *in primis* dalle cartelle cliniche a disposizione dell'Istituto Auxologico in fase di cura del paziente.

i. Recupero delle cartelle cliniche ospedaliere del gruppo di Studio

I dati personali riferibili al singolo paziente sono stati estratti dalle cartelle cliniche, già presenti presso il Titolare prima della messa in opera dello Studio. La custodia delle cartelle cliniche viene effettuata all'interno della struttura, ma anche all'esterno. Con riferimento agli spazi esterni, l'archiviazione e la digitalizzazione delle cartelle cliniche è stata affidata a Normadec Digital S.r.l.. Nel dettaglio, le cartelle cliniche sono state organizzate nel seguente modo: dall'inizio del 2016 le cartelle hanno iniziato a essere custodite e scannerizzate, tra il 2001 e il 2015 è la struttura del Titolare che gestisce tali dati e prima del 2001 le cartelle sono ubicate nell'archivio esterno di Normadec Digital S.r.l. offrendo il solo servizio di custodia.

Il trattamento ha inizio nel momento in cui i dati clinici già raccolti e archiviati vengono estratti dalla cartella clinica e resi disponibili, in forma pseudonimizzata, per le finalità di ricerca previste dal protocollo di studio.

I dati personali riferibili al singolo paziente sono stati originariamente raccolti dall'Istituto Auxologico per svolgere tutte le necessarie attività di analisi e di cura. Al fine di pseudonomizzarli, ai dati sono stati assegnati dei codici alfanumerici ("ID"). I dati sono protetti da password.

L'accesso alle cartelle cliniche depositate da Normadec è differenziato tra: a) richiesta di sola lettura: sono autorizzati tutti i medici ai quali, dopo richiesta, sono state rilasciate le credenziali di accesso a Normadec; b) richiesta di lettura e stampa: in tal caso sono autorizzati il Direttore Sanitario (di seguito anche "DS"), la segreteria del DS e gli operatori dell'archivio con le credenziali personali di accesso a Normadec. Si precisa che la stampa richiede sempre il preventivo coinvolgimento e l'autorizzazione del DS.

ii. Creazione del database

I singoli dati estratti sono poi riportati in un file excel protetto da doppia password di accesso, in particolare i soli dati necessari e utili ai fini dello Studio (v. *supra* i dati personali dei pazienti trattati).

L'identificazione dei pazienti è effettuata attraverso codificazioni derivanti da codici di pseudonimizzazione assegnati in fase di rilevazione e registrati nell'apposito *database*.

iii. Elaborazione statistica dei dati

I dati personali raccolti sono sottoposti ad un'analisi statistica volta a valutare una serie di indici derivati dai parametri antropometrici, biochimici e clinici sopra descritti: triponderal mass index (TMI), A Body Shape Index (ABSI), rapporto circonferenza vita/statura (WtHR), Visceral Adiposity Index (VAI), CardioMetabolic Index (CMI) rapporto Colesterolo Totale/HDL (CT/HDL) e rapporto Trigliceridi/HDL (TG/HDL).

iv. Stesura di lavoro scientifico da pubblicare su rivista indicizzata

I dati pubblicati sulle riviste scientifiche sono completamente anonimi, non vi è modo per chi consulta i lavori scientifici di risalire all'identità del paziente.

g. Destinatari dei dati

I dati sopra elencati sono trattati unicamente dai soggetti appositamente autorizzati secondo le procedure interne dell'Istituto Auxologico. Nello specifico sono soggetti autorizzati dall'Istituto Auxologico a trattare i dati personali dei pazienti partecipanti agli studi clinici: (*i*) i medici e professionisti incaricati della prestazione sanitaria, (*ii*) i *principal investigators* (PI) del singolo Studio, (*iii*) i membri del gruppo di ricerca del PI (specificatamente per la raccolta dei dati e la loro elaborazione e analisi) e se necessario, (*iv*) dal personale dei sistemi informativi e/o dei

fornitori dei servizi di assistenza e manutenzione ai *software*, per le attività di assistenza e manutenzione dei sistemi informatici utilizzati.

I dati trattati dall'Istituto Auxologico per il perseguimento delle finalità di ricerca sono trasmessi o eventualmente acceduti ai soggetti coinvolti a vario titolo nella sperimentazione, in funzione del ruolo e del tipo di studio, quali:

- Autorità sanitarie competenti: istituzioni preposte alla valutazione e verifica della conformità dello studio per le materie di propria competenza

I responsabili del trattamento coinvolti nei processi di ricerca clinica sono vincolati per contratto stipulato ai sensi dell'art. 28 del Regolamento UE 2016/679. Qualora l'Istituto Auxologico dovesse avvalersi di un sistema informativo non proprio, o di prestazioni di analisi *in service*, nel contratto con la struttura individuata sono espressamente indicati i compiti affidati al responsabile del trattamento, le misure di sicurezza da garantire ed adottare, la finalità del conferimento dei dati, la durata del trattamento ed ogni altro obbligo da imporsi secondo lo specifico incarico conferito.

In relazione alle operazioni di trattamento in esame, non è previsto il trasferimento di dati personali al di fuori dello Spazio Economico Europeo (SEE)

h. Asset coinvolti

- *MedArchiver*
- *Postazioni aziendali e rete aziendale*

4. Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità

a. Adeguatezza, pertinenza e limitazione a quanto necessario rispetto alle finalità (principio di minimizzazione dei dati)

In ogni studio clinico, l'Istituto Auxologico si impegna a raccogliere i soli dati utili e quindi pertinenti e necessari per lo svolgimento delle attività di ricerca descritte nei protocolli in conformità con il principio di minimizzazione.

Il principio di minimizzazione dei dati è garantito dall'applicazione rigorosa del protocollo clinico, che individua nello specifico le aree di intervento e quindi le informazioni necessarie per lo svolgimento dello Studio. Nelle banche dati sono registrati e raccolti solo i dati indicati richiesti dal protocollo clinico e finalizzati al raggiungimento dell'obiettivo dello Studio. Nel protocollo sono definiti in maniera precisa i criteri di inclusione o esclusione dallo Studio, pertanto vengono inclusi soltanto i dati che corrispondono al profilo ricercato. I dati raccolti saranno trattati esclusivamente per le finalità dello Studio.

Vengono raccolti solo i dati strettamente necessari alla realizzazione dello Studio. Inoltre, i dati sono pseudonimizzati e le chiavi di lettura di difficile accesso.

Al momento della cancellazione dei dati da parte di Istituto Auxologico, verrà eliminata altresì la chiave di lettura del dato pseudonimizzato, e le informazioni raccolte saranno totalmente anonimizzate e non verranno più qualificate come dati personali.

Nel protocollo sono definiti in maniera precisa i criteri di inclusione o esclusione dallo Studio, pertanto vengono inclusi soltanto i dati che corrispondono al profilo ricercato.

b. Finalità del trattamento specifiche, esplicite e legittime (principio di limitazione della finalità)

I dati sono trattati per finalità di ricerca scientifica.

Le finalità sono esplicite perché dichiarate nelle informative e nei documenti predisposti per lo svolgimento e l'esecuzione dello Studio.

L'attività di terapia effettuata dall'Istituto Auxologico e la gestione della relativa documentazione clinica è effettuata sotto la responsabilità dell'Istituto Auxologico, in qualità di Titolare del trattamento, in un processo separato che alimenta quello della ricerca clinica.

c. *I dati sono esatti e se necessario, aggiornati? (principio di esattezza)*

La garanzia di esattezza e aggiornamento dei dati è garantita dall'esecuzione del protocollo clinico. I dati del partecipante sono periodicamente aggiornati per tutta la durata dello Studio fino al termine delle procedure descritte nel protocollo. Con riferimento allo Studio, in quanto retrospettivo, l'esattezza dei dati è relativa al momento in cui i dati sono stati raccolti, così come conservati in cartella clinica e nei *software* dell'Istituto Auxologico e non vi è necessità di aggiornamento.

Siccome la fonte dei dati è costituita dai documenti clinici formati per finalità di cura i dati non sono modificabili, diversamente da quanto accade per gli studi prospettici dove i dati vengono trattati su dei *repository* costruiti *ad hoc*.

d. *Liceità, correttezza e trasparenza nei confronti dell'interessato*

I soggetti interessati ricevono l'informativa al momento del loro ingresso presso l'Istituto Auxologico. Al servizio di accettazione della struttura infatti i soggetti interessati che si sottopongono a degli esami e analisi sanitari sono informati circa la natura dei loro dati trattati e delle finalità corrispondenti, ivi compresa la finalità di ricerca e sviluppo scientifico a partire dai loro dati.

L'informativa resa agli interessati contiene tutti gli elementi che descrivono le modalità di raccolta; pertanto, si ritiene che le procedure siano trasparenti e che non si possano verificare situazioni di intrusività nella sfera personale non conosciuta o non condivisa.

Il trattamento dei dati personali, effettuato nell'ambito di ricerca, nelle sue diverse forme è descritto in forma chiara e intellegibile, rispettando i requisiti previsti dall'art. 13 del GDPR.

i. I soggetti interessati sono informati del trattamento?

Prima della raccolta dei dati, i pazienti vengono debitamente informati dal Titolare tramite un'informativa esposta agli sportelli dell'ufficio accettazione e consegnata in formato cartaceo dal personale preposto al momento dell'accettazione in seno alla struttura e comunque sempre disponibile nella sezione *privacy* del sito istituzionale www.auxologico.it. I soggetti interessati sono quindi informati della possibilità di riutilizzo dei loro dati contenuti nelle cartelle cliniche per finalità di ricerca scientifica (v. sezione "*trattamenti non soggetti a consenso*" punto c) "***Finalità di ricerca scientifica:*** *è dimostrato come la ricerca scientifica migliori la qualità delle cure. Quale Istituto di Ricovero e Cura a Carattere Scientifico (IRCCS), l'Istituto Auxologico Italiano svolge numerosi studi clinici che permettono di migliorare nel lungo termine le conoscenze in ambito scientifico e di sviluppare tecniche di diagnosi e cura sempre più efficienti. Ciò implica il trattamento dei Suoi dati personali raccolti per la pratica clinica a cui Lei si sottopone. Questo tipo di trattamento si fonda sul disposto dell'art. 110 bis comma 4 del D.lgs. 196/2003, integrato con le modifiche introdotte dal D.lgs. n. 101 del 10 agosto 2018 (Codice della privacy) che permette agli IRCCS, in ragione del carattere strumentale dell'attività di assistenza sanitaria, di utilizzare tali dati nonché l'eventuale materiale biologico raccolto nel medesimo contesto per promuovere progetti di ricerca scientifica.*")

Per gli studi retrospettivi come il presente, l'Istituto assolve agli obblighi di trasparenza verso i pazienti attraverso la pubblicazione sul proprio sito web istituzionale del Modulo Informativo specifico dello studio, che descrive in dettaglio le finalità della ricerca, la natura retrospettiva dell'analisi. L'Istituto garantisce la massima visibilità a tale modulo nella sezione dedicata alla ricerca scientifica e alla trasparenza, assicurando che i diritti ex artt. 15-22 GDPR siano esercitabili in ogni momento, nonostante il riuso dei dati avvenga senza la raccolta del consenso preventivo, in virtù della base giuridica fornita dal combinato disposto degli artt. 9 par. 2 lett. j) del GDPR e 110-bis del D.lgs. 196/2003.

Inoltre i soggetti interessati potranno essere a conoscenza degli studi retrospettivi effettuati tramite la pubblicazione sul sito di una valutazione d'impatto come la presente.

ii. Come vengono esercitati i diritti da parte degli interessati?

In qualunque momento un soggetto interessato potrà contattare il Titolare e il rispettivo DPO all'indirizzo indicato nell'informativa resa al momento della raccolta dei dati da parte dell'Istituto Auxologico, indirizzo postale oppure tramite indirizzo mail o PEC e quindi ottenere conferma che sia o meno in corso un trattamento dei suoi dati personali e nel caso richiedere una copia dei dati trattati dal Titolare. L'interessato può esercitare i diritti di accesso e

portabilità facendo richiesta a dpo@auxologico.it, oppure mezzo fax 02619112204, oppure con raccomandata RR indirizzata alla sede legale in Milano, via L. Ariosto n.13. Generalmente, di fronte a una richiesta di portabilità o accesso, il DPO informa l'ufficio amministrazione di sistema e/o i sistemi informativi i quali raccolgono le informazioni che Istituto Auxologico possiede sull'interessato e creano un *file* Excel con copia dei dati. Il *file* verrà poi protetto da password criptato e inviato all'interessato.

Il DPO e la struttura dispongono di sufficienti canali di comunicazione per dare celere riscontro alle domande di esercizio dei diritti da parte dei soggetti interessati. Le domande di esercizio dei diritti sono trattate entro il termine di 30 giorni e caricate sul portale interno dell'Istituto Auxologico, "*Privacy Encoder*", per tenere traccia delle domande effettuate, il tipo di richiesta, le richieste dell'Istituto Auxologico circa la fornitura di documentazione ulteriore (ad es. il codice fiscale) per evacuare la richiesta e rimuovere i dati concernenti i pazienti dai sistemi gestionali e di archivio interni alla struttura.

Con riferimento al diritto di cancellazione si precisa che esso è esercitabile limitatamente: gli istituti privati sono soggetti alla legge che li obbliga alla conservazione illimitata delle cartelle cliniche.

Il trattamento dei dati non viene effettuato né sulla base del consenso dell'interessato ai sensi dell'art. 6, comma 1, lettera a) o dell'art. 9, comma 2, lettera a) oppure l'esecuzione di misure pre-contrattuali o contrattuali secondo la lettera b) dell'art. 6 del GDPR. Quindi, nella misura del possibile e del tecnicamente fattibile, qualora l'interessato lo richieda, l'Istituto Auxologico comunicherà in un formato strutturato, di uso comune e leggibile i dati ai sensi dell'articolo 20 del GDPR.

Per quanto riguarda il diritto alla revoca del consenso, questo non è esercitabile nel momento in cui il trattamento non si basa sul consenso dell'interessato. Invece in qualunque momento, l'interessato potrà contattare il Titolare tramite le modalità descritte *supra* per esercitare il proprio diritto di rettifica dei dati, di cancellazione e di limitazione e di opposizione, nei limiti previsti dalla legge o dall'interesse legittimo del Titolare a difendersi in sede stragiudiziale o giudiziale.

Al fine di identificare correttamente l'interessato, al momento della richiesta di esercizio del diritto, a questi viene richiesta di fornire un documento d'identità non essendo spesso chiara l'identità dello stesso dal solo indirizzo e-mail, ed essendovi casi di omonimia. Pertanto, una non corretta identificazione dell'interessato genererebbe il rischio di fornire l'accesso a dati altrui. La comunicazione garantisce, dunque, un corretto esercizio dei diritti, ed è giustificata anche alla luce del fatto che essa rappresenta conferma di un dato di cui il Titolare è già in possesso; pertanto non vengono richiesti dati ulteriori rispetto a quelli già oggetto di trattamento da parte del Titolare.

5. Valutazione dei rischi per i diritti e le libertà degli interessati

a. *I rischi possibili connessi al trattamento – considerazioni generali*

Il concetto di rischio è rappresentato dalla combinazione dei due seguenti elementi:

- La probabilità che avvenga il danno
- Le conseguenze di questo danno, cioè la gravità

Le violazioni del GDPR possono causare danni "materiali" o "immateriali". Tra questi ultimi possono rientrare: la perdita del controllo sui dati personali, la limitazione dei diritti, la perdita di riservatezza; tra quelli materiali, invece, rientrano non solo le violazioni delle misure di sicurezza ma anche le perdite finanziarie e gli altri rischi economici.

Con riferimento al trattamento in esame, sono state individuate 3 tipologie di rischio a cui i dati personali potrebbero potenzialmente essere esposti, in particolare:

(i) Rischi interni (ossia arrecati da dipendenti, collaboratori del Titolare);
(ii) Rischi esterni (ossia imputabili, ad esempio, al trattamento da parte di soggetti terzi);
(iii) Rischi imputabili ad agenti esterni, quali, per esempio: incidenti informatici e disastri naturali.

b. *Rischi connessi al trattamento dei dati personali nel quadro dello Studio*

Un rischio sarebbe l'***accesso illegittimo ai dati.***

I principali impatti sugli interessati se il rischio si dovesse concretizzare sarebbero la perdita della riservatezza, la perdita sul controllo dell'utilizzo dei dati e il riutilizzo illecito dei dati personali acquisiti.

Le principali minacce che potrebbero concretizzare il rischio sarebbero la sottrazione delle credenziali di accesso, un attacco al sistema informatico aziendale e l'intercettazione delle comunicazioni.

Le fonti di rischio sarebbero il comportamento improprio del personale interno o esterno o la presenza di un attaccante esterno.

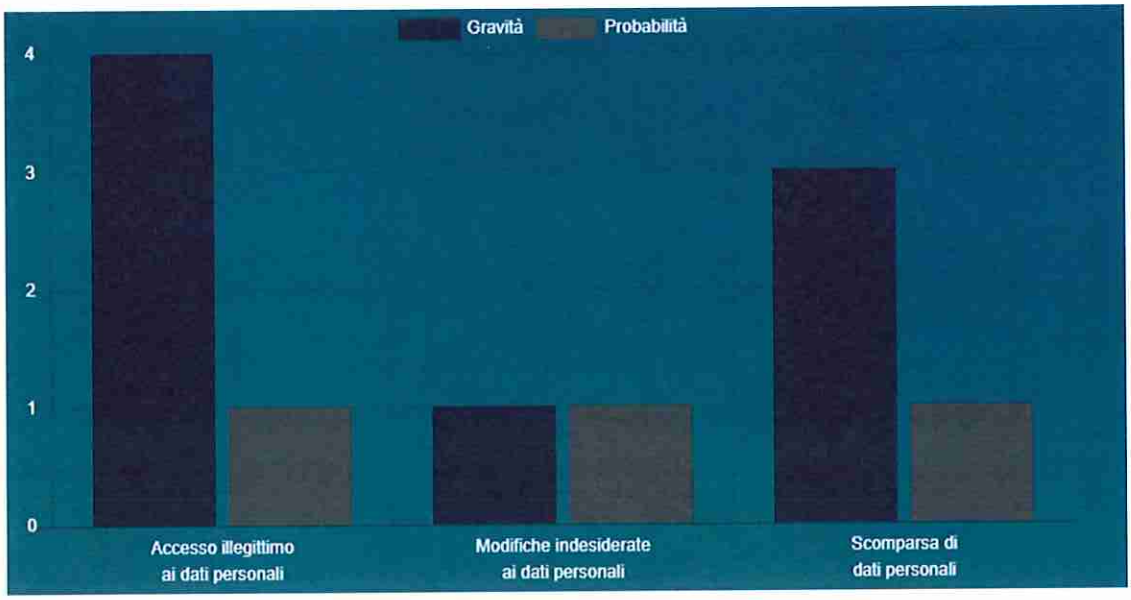
Misure di mitigazione di questi rischi (controllo degli accessi logici, gestione delle postazioni, il *backup*, il controllo degli accessi fisici, la sicurezza dell'*hardware*, gestionale del personale, la lotta contro il *malware*, la pseudonimizzazione, la gestione degli incidenti di sicurezza e delle violazioni dei dati personali, la minimizzazione dei trattamenti dei dati personali.

La gravità del rischio sarebbe importante, nonostante la natura retrospettiva dello Studio condotto in seguito all'erogazione delle prestazioni di cura, le misure di minimizzazione, pseudonimizzazione e sicurezza dell'*hardware*, la sicurezza dei canali informatici e la formazione del personale. La gravità del rischio di perdita di controllo dei dati e della riservatezza residuo risulta comunque elevato in quanto l'eventuale accesso ai dati dei pazienti in chiaro, comprometterebbe la loro riservatezza e determinerebbe la mancanza di controllo sull'utilizzo dei dati, impatti materiali e immateriali significativi vista la categoria particolarmente vulnerabile dei soggetti interessati coinvolti nel trattamento.

La probabilità del rischio resterebbe comunque limitata, date le misure di minimizzazione, di pseudonimizzazione, di *backup* e controllo degli accessi logici, di sicurezza dei canali informatici, di cifratura, credenziali forti, quindi il rischio di eventuale accesso illegittimo dei dati residuale risulta limitato.

Ulteriore rischio sarebbe la ***modifica indesiderata dei dati,*** anche se non vi sarebbero particolari impatti sugli interessati se questo rischio dovesse concretizzarsi. Il rischio potrebbe concretizzarsi in caso di errata compilazione della CRF. Attraverso misure di mitigazione quali il *backup* dei dati, la gravità e la probabilità del rischio risultano particolarmente trascurabili e gli eventuali impatti di una modifica interessano la buona riuscita dello Studio e non i soggetti interessati e inoltre l'evento sarebbe improbabile vista l'alta specializzazione del personale di ricerca.

Per quanto riguarda la ***perdita dei dati,*** gli impatti sarebbero la perdita della riservatezza e sul controllo dell'utilizzo e sfruttamento dei dati. Le minacce che potrebbero consentire la materializzazione del rischio sarebbero la perdita delle credenziali di accesso ai dispositivi aziendali, o la loro sottrazione, un attacco al sistema informatico aziendale. La gravità del rischio sarebbe importante data la natura retrospettiva dello Studio condotto in seguito all'erogazione delle prestazioni di cura. Ciononostante, alla luce delle misure pianificate la probabilità del rischio risulterebbe limitata, date le misure di minimizzazione, di archiviazione e sicurezza dei canali informatici.



6. Le misure previste per affrontare i rischi, incluse le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto degli interessi legittimi degli interessati e delle altre persone in questione

La gestione dei rischi è l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

Come noto, il GDPR individua specifiche misure di sicurezza da adottare per garantire la tutela dei diritti e le libertà dei soggetti interessati. In particolare:

(i) la pseudonimizzazione e la cifratura dei dati personali;
(ii) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
(iii) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
(iv) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

I dati raccolti all'interno dello Studio a partire dalle cartelle cliniche dei pazienti, vengono registrati in uno specifico *database* con accesso limitato al PI e ai suoi delegati tramite credenziali personali.

I dottori, *principal investigators*, trattano i dati dei pazienti esclusivamente in forma pseudonimizzata, in tal modo l'Istituto Auxologico garantisce l'assoluta riservatezza dei dati dei pazienti.

I dati pseudonimizzati sono trasferiti, per motivi di pubblicazioni di ricerche e studi, tramite un file in formato *excel* protetto da nome utente e *password*.

a. Le misure di sicurezza

- i dati vengono conservati su infrastruttura IT di proprietà dell'Istituto Auxologico (sicurezza della infrastruttura *in house*);
- l'infrastruttura IT è costantemente monitorata per ridurre al minimo gli incidenti di sicurezza informatica (sicurezza dei canali informatici, gestione delle vulnerabilità);
- misure applicate sui dati (crittografia e pseudonimizzazione);

- l'accesso ai dati è controllato tramite la gestione degli accessi con definizione degli appropriati permessi (controllo degli accessi logici, tracciabilità, sicurezza dei dispositivi di accesso dell'utente);
- i dati saranno soggetti alle esistenti politiche di *backup* dell'Istituto Auxologico;
- l'efficacia delle misure verrà verificata su base annuale come da politiche di gestione interne dell'Istituto Auxologico (gestione degli incidenti di sicurezza e delle violazioni dei dati personali);
- Contratti con i responsabili del trattamento dei dati personali.

Per quanto riguarda la conservazione digitale, l'Istituto Auxologico si avvale di MedArchiver tramite l'omonimo sistema, che fornisce una conservazione digitale a norma, assicurando l'integrità e l'autenticità dei documenti nel tempo. Le misure di sicurezza adottate da MedArchiver per garantire la protezione dei dati comprendono la protezione fisica e logica dei sistemi di conservazione, la gestione dei *log* di accesso e la duplicazione dei documenti.

Gestione del personale: il personale dell'Istituto Auxologico è debitamente formato con cadenza periodica sulla normativa in materia di protezione dei dati personali, con un focus specifico in funzione dei trattamenti svolti. Inoltre il personale nominato autorizzato al trattamento dei dati personali ex art. 29 GDPR, riceve dal Titolare le istruzioni per il trattamento ed è messo a conoscenza delle procedure interne che disciplinano determinati trattamenti e che sono sempre consultabili tramite apposite aree del sistema informativo aziendale.

Il personale viene adeguatamente formato in merito alle attività di trattamento e ai sistemi di sicurezza da adottare.

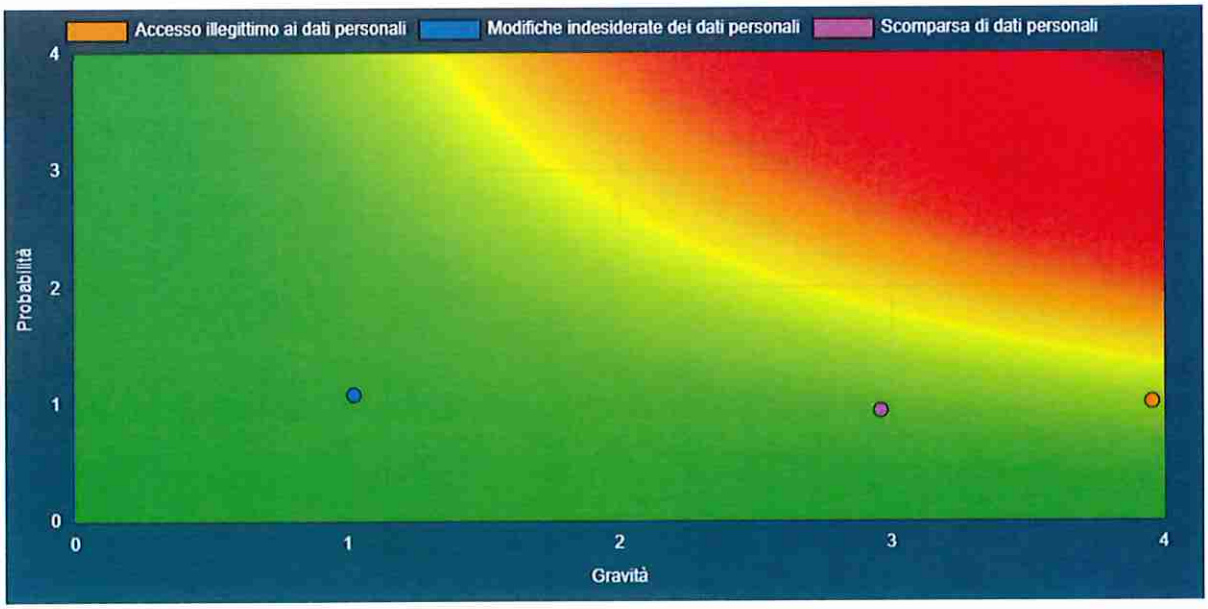
Per tale scopo:

- sono redatti specifici regolamenti interni
- vengono effettuate sessioni formative
- vengono effettuati audit presso le strutture interessate

b. Il livello di rischio

Alla luce di quanto esposto, si ritiene che il livello di rischio per i diritti e le libertà dei soggetti interessati sia basso.

Inoltre, ai sensi dell'art.36 del GDPR, non si ritiene necessario il ricorso alla consultazione dell'Autorità Garante per la Protezione dei Dati Personali ("Garante") e si decide di procedere in tal senso.



7. Parere del DPO

Il DPO valuta positivamente conclusa la presente DPIA relativa al descritto Studio di ricerca retrospettivo.

Il DPO, considerate le misure determinate per garantire l'impossibilità di ricondurre il dato ad una persona fisica e le garanzie adottate per tutelare i diritti e le libertà degli interessati, concorda nel ritenere che il trattamento presenti un livello di rischio basso.

Si raccomanda all'Istituto Auxologico di monitorare qualsiasi mutamento nel previsto trattamento dei dati e di descriverlo all'interno della presenta DPIA. A tal proposito, andranno previste verifiche periodiche volte ad accertare che l'architettura del progetto non presenti delle modifiche che richiedano un'ulteriore valutazione.

Qualora si verificassero mutamenti che comportino un innalzamento del livello di rischio, si raccomanda di procedere con la Consultazione Preventiva al Garante, ai sensi di quanto previsto dall'Art.36 GDPR.

Il Presidente e Legale Rappresentante