RAPPORTO
DATA PROTECTION IMPACT ASSESSMENT (DPIA)
"STUDI OSSERVAZIONALI RETROSPETTIVI"

Autore/i: DPO/Supporto Specialistico

Rivisto da UOC Privacy – Trasparenza e Integrità

Accettato da: Direzione Generale

STORICO DELLE REVISIONI			
Vers.	**Data di rilascio**	**Motivo della revisione**	**Autore**
1.0	12/05/2025	Prima Versione	DPO/Supporto Specialistico
L'ultima revisione sostituisce qualsiasi revisione precedente.			

A.O.R.N.
"AZIENDA OSPEDALIERA DEI COLLI"
Monaldi-Cotugno-CTO

Indice

1 INTRODUZIONE

Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 [1] (di seguito sinteticamente indicato come "Regolamento" o "GDPR") stabilisce norme relative sia alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, sia alla libera circolazione di tali dati. Tali norme sono finalizzate a proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali e la libera circolazione dei dati personali nell'Unione Europea.

Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate, il Regolamento (cfr. art. 35) obbliga i titolari a svolgere un Data Protection Impact Assessment (DPIA) o "Valutazione di impatto sulla protezione dei dati" prima di darvi inizio. Qualora in assenza di misure la DPIA indica che il trattamento presenterebbe un rischio elevato per la tutela dei diritti dell'interessato, il titolare consulta il Garante per la protezione dei dati personali circa gli interventi necessari per attenuare il rischio (rischio residuo elevato).

La DPIA è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per ridurli. La valutazione d'impatto sulla protezione dei dati è uno strumento importante di responsabilizzazione in quanto sostiene il titolare del trattamento non soltanto nel rispettare i requisiti del Regolamento, ma anche nel dimostrare che sono state adottate misure appropriate.

In linea con quanto previsto dal Regolamento e con le relative disposizioni per l'adeguamento della normativa nazionale [2], la Struttura Sanitaria mantiene un registro delle attività di trattamento [7] ed effettua una Data Protection Impact Assessment sulla protezione dei dati personali per i trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

1.1 SCOPO DEL DOCUMENTO

Come sopra indicato il trattamento dei dati personali deve avvenire nel rispetto della normativa applicabile in materia di protezione dei dati personali e, in particolare, delle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito, il "Regolamento" o "GDPR") e del D.lgs.n. 196 del 30 giugno 2003 e ss.mm.ii.

I dati, inoltre, devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che il trattamento non sia incompatibile con tali finalità e, comunque, devono essere "adeguati, pertinenti e limitati a quanto necessario alle finalità per le quali sono trattati" (principi della limitazione della finalità e di minimizzazione dei dati - art. 5, par. 1, lett. b) e c) del Regolamento). Devono, altresì, essere "trattati in modo lecito corretto e trasparente" (principio di liceità, correttezza e trasparenza) ed "in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti" (principio di integrità e riservatezza) (art. 5, par. 1, lett. a) e f) del Regolamento).

Il Regolamento prevede poi che il titolare del trattamento valuti i rischi che un trattamento può determinare sui diritti e libertà fondamentali degli interessati e, conseguentemente, metta in atto "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio", tenendo conto, tra l'altro "della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" (art. 32 del Regolamento).

Ciò premesso, lo scopo del presente documento è quello di fornire una valutazione del rischio che il trattamento dei dati, relativo all'attività di conduzione di uno **Studio Osservazionale Retrospettivo**, potrebbe avere sui diritti e sulle libertà dei soggetti interessati, al fine di valutarne la necessità e la proporzionalità.

Tale valutazione è necessaria, inoltre, per consentire la gestione dei rischi derivanti dal trattamento stesso, anche attraverso la programmazione di misure organizzative e tecniche idonee a garantire il rispetto delle disposizioni in materia di trattamento dei dati personali.

1.2 AMBITO DI APPLICAZIONE

Ogni Studio Osservazionale, per poter essere organizzato e condotto, viene sottoposto all'autorizzazione del Comitato Etico competente tramite la redazione di un apposito protocollo corredato di tutta la documentazione clinica e amministrativa necessaria tra cui, ove previsto, un documento informativo per l'acquisizione del consenso alla partecipazione da parte del paziente.

Di norma, la conduzione di uno **Studio Osservazionale Retrospettivo** avviene sulla raccolta dei dati clinici dopo che i pazienti sono stati sottoposti a trattamento o terapia, a partire dalle loro cartelle cliniche che pertanto, solitamente hanno come obiettivo quello di rispondere ad un quesito clinico che riguarda la terapia di routine. Ovvero, i dati oggetto dello studio sono già presenti nei sistemi del titolare del trattamento e sono stati raccolti in occasione delle prestazioni sanitarie precedentemente erogate.

Tale aspetto comporta che numerosi pazienti partecipanti allo studio potrebbero essere deceduti o risultare non reperibili per cui potrebbe non risultare possibile, da parte del titolare, informarli e raccogliere il proprio consenso al trattamento dati. In tal caso il titolare del trattamento, ai sensi dell'art. 110 comma 1 del D.Lgs. 196/2003, integrato con le modifiche introdotte dal D.Lgs. 101/2018 in adeguamento al Regolamento UE 69/2016 (GDPR), nonché successivamente novellato dall'art. 44, comma 1-bis della legge 29 aprile 2024, n. 56, di conversione del d.l. n. 19 del 2 marzo 2024, **potrà assumere che non è necessario il consenso al trattamento dati dei soggetti partecipanti allo studio.**

Tuttavia, nel rispetto delle "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice - 9 maggio 2024" (provvedimento n. 289 del 9 maggio 2024), il titolare del trattamento AO dei Colli, nell'ottica di adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, oltre ad acquisire il parere favorevole del competente comitato etico a livello territoriale sul protocollo dello studio, ha disposto che vengano accuratamente motivate e documentate, all'interno del suddetto protocollo, la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati e quindi acquisire il consenso, risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. Sempre nell'ottica di tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il titolare del trattamento, in accordo con quanto predisposto nelle suddette regole deontologiche, ha disposto, inoltre, di condurre, ai sensi dell'art. 35 del Regolamento, la presente **Valutazione d'Impatto sulla Protezione dei dati** (Data Protection Impact Assessment), disponendone, altresì, la pubblicazione sul proprio sito aziendale www.ospedalideicolli.it/privacy/, nonché di darne comunicazione al Garante.

A tale proposito si rappresenta che nella conduzione della presente DPIA assume fondamentale importanza la funzione attribuita al Protocollo dello Studio che, oltre alla obbligatoria descrizione del processo di ricerca, deve identificare ed illustrare ampiamente le misure tecniche ed organizzative che devono essere necessariamente adottate durante lo svolgimento dello Studio al fine di garantire un adeguato livello di sicurezza per la tutela e protezione dei dati personali e particolari dei soggetti arruolati. Nello specifico si evidenzia che il rispetto delle misure dettagliate nel capitolo 2 "DEFINIZIONE DEL

CONTESTO" del presente documento, e riportate nel protocollo è condizione essenziale per assicurare un livello di rischio accettabile.

Per quanto sopra e, tenendo conto della comune finalità, tipologia e caratteristica degli studi osservazionali retrospettivi promossi per conto del Titolare del trattamento dati da parte degli sperimentatori principali, della rigorosa osservanza da parte degli stessi delle disposizioni del Titolare in riferimento alle modalità di conduzione e agli standard operativi adottati, nonché dell'utilizzo delle medesime risorse tecniche ed organizzative adottate a supporto dello sviluppo dei singoli studi, si può assumere che la presente DPIA, salvo casi specifici, possa essere ritenuta applicabile agli studi osservazionali retrospettivi operati dall'Azienda (**art. 35 del Regolamento: "Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi")**.

1.3 DEFINIZIONI E ACRONIMI

Categorie particolari di dati personali	Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 GDPR).
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
Dati relativi alla salute	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
DPIA	Data Protection Impact Assessment (art. 35 del GDPR).
DPO	Data Protection Officer.
GDPR	Regolamento Generale per la Protezione dei Dati.

Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, 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.
Pseudonimizzazione	Il trattamento dei dati personali 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.
RDP	Responsabile della Protezione dei Dati.
Referto online	Possibilità di accedere al referto tramite modalità digitali (Fascicolo sanitario elettronico, sito Web, posta elettronica anche certificata, supporto elettronico).
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Titolare del trattamento	La 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Violazione dei dati personali	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Studio osservazionale Retrospettivo	Lo studio retrospettivo è uno studio disegnato in modo da raccogliere ed elaborare i dati relativi a pazienti già sottoposti ad una strategia terapeutica, indagine clinica e/o attività di normale pratica clinica, mediante raccolta ed analisi secondaria dei relativi dati clinici.

1.4 RIFERIMENTI

[1] Regolamento (UE) 2016 del Parlamento Europeo e del Consiglio, del 27 Aprile 2016, relativo alla protezione delle persone con riguardo al trattamento dei dati personali – Regolamento Generale sulla Protezione dei Dati (GDPR) e s.m.i.

[2] D.lgs 10 agosto 2018, n. 101. "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)"

[3] D.Lgs. 30 Giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e s.m.i.

[4] Provvedimento Garante Privacy del 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

[5] "Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali – 24 luglio 2008 G.U. n. 190 del 14 agosto 2008" del Garante per la Protezione dei Dati Personali.

[6] Provvedimento Garante Privacy n. 289 del 9 maggio 2024 "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice - 9 maggio 2024".

[7] "Registro delle attività di trattamento" della Struttura Sanitaria.

2. DEFINIZIONE DEL CONTESTO

Il presente capitolo definisce il contesto del trattamento dei dati personali in esame, in termini di:

- Responsabilità del trattamento;
- Descrizione del trattamento e delle finalità;
- Principi fondamentali – diritti degli interessati
- Descrizione-analisi misure tecniche-organizzative adottate.

2.1 RESPONSABILITA' DEL TRATTAMENTO

Titolare del trattamento	AO Dei Colli Monaldi-Cotugno-CTO
Rappresentante	DG
Contitolare del trattamento	non applicabile
Responsabile della Protezione dei Dati (DPO)	Dottoressa Maria Mauro
Referente	Direttori UOC/UOSD Ufficio di Segreteria del Comitato Etico

2.2 DESCRIZIONE DEL TRATTAMENTO

DESCRIZIONE DEL TRATTAMENTO		Valutazione
Denominazione del trattamento	Studi osservazionali retrospettivi. La natura, le caratteristiche e l'organizzazione dello studio sono ampiamente documentate nel corrispondente Protocollo redatto nel rispetto delle linee guida, regolamenti e disposizioni previste dall'Autorità Regolatoria, ovvero Agenzia Italiana del Farmaco (AIFA), da eventuali decreti Ministeriali, nonché secondo le GCP (Good Clinical Practice) per condurre studi osservazionali ed è approvato dal CET.	**N.A.**
Indicare la finalità del trattamento	Le finalità di trattamento sono identificate nel fine di ricerca scientifica e/o statistica avente ad oggetto il miglioramento della diagnosi e della cura delle patologie di cui sono affetti i soggetti partecipanti allo studio, nonché l'efficienza dei	**N.A**.

	servizi erogati. Più nello specifico la finalità scientifica dello studio è quella di valutare la strategia di cura attualmente in utilizzo per il trattamento delle suddette patologie allo scopo di verificarne il grado di miglioramento della risposta clinica, anche in termini della qualità di vita del paziente, misurato attraverso specifici questionari. La valenza scientifica dello studio viene valutata dal comitato etico competente il cui assenso sarà condizione indispensabile per l'inizio dello studio.	
Indicare le tipologie di dati oggetto del trattamento, specificando ogni tipologia di dato	Dati comuni: dati anagrafici e identificativi, età, genere, dati sullo stile di vita Dati appartenenti a categorie particolari: dati clinici personali attinenti allo stato di salute fisica o mentale, eventuali dati di familiari, dati genetici idonei a rivelare informazioni relative allo stato di salute, dati che rilevano l'origine razziale o la vita e l'orientamento sessuale.	**N.A.**
Indicare le tipologie di interessati al trattamento	Il numero di pazienti affetti da patologie trattate attraverso la strategia di cura oggetto dello studio è espressamente indicato nel Protocollo dello studio. La raccolta dei dati clinici avviene dopo che i pazienti sono stati sottoposti a trattamento o terapia, a partire dalle loro cartelle cliniche che pertanto, solitamente, hanno come obiettivo quello di rispondere ad una strategia terapeutica, indagine clinica e/o attività di normale pratica clinica, mediante raccolta ed analisi secondaria dei relativi dati clinici. Nello specifico tali dati, come più dettagliatamente descritto nel Protocollo dello studio, sono già presenti nei sistemi del titolare del trattamento perché raccolti in occasione delle prestazioni sanitarie precedentemente erogate.	**N.A.**
Indicare i soggetti interni che partecipano al trattamento quali persone espressamente designate o autorizzate e se queste siano state adeguatamente istruite sul trattamento	Le attribuzioni di responsabilità nel trattamento dei dati sono connesse con il ruolo rivestito dai diversi soggetti all'interno della ricerca clinica. Il promotore dello studio è l'AO dei Colli, Titolare del trattamento, e si assume di conseguenza l'onere di verificare e controllare che i dati siano trattati nel rispetto della normativa. Il centro sperimentatore, anche Sperimentatore principale (PI) è, solitamente, il Responsabile della UO che materialmente conduce lo studio o, eventualmente, un altro soggetto afferente a tale UO. Nello specifico, lo Sperimentatore principale del centro, e nel caso di studio multicentrico quello di ogni singolo centro partecipante, verrà nominato dal proprio Titolare quale Delegato interno per il trattamento dei dati personali dello Studio - ai sensi e per gli effetti dell'art. 2-quaterdecies del Codice Privacy, mentre i Co-Sperimentatori, gli statistici e gli informatici e tutti coloro che possono accedere ai dati personali dello Studio sono nominati autorizzati al trattamento dati ai sensi dell'art. 29 del GDPR e dell'art. 2-	**Accettabile**

	quaterdecies sopracitato. Come indicato nel Protocollo a ognuno dei soggetti sopra indicati sono fornite apposite istruzioni scritte e viene fatto loro assumere l'impegno a conformarsi alle Regole deontologiche, nonché alle regole di condotta per il trattamento dei dati dei pazienti adottate dal Centro. È cura dello/degli Sperimentatore/i principale/i individuare adeguati livelli di accesso (integrale o parziale) ai dati e alle informazioni dello Studio da parte dei Co-Sperimentatori.	
Indicare eventuali soggetti esterni che partecipano al trattamento quali titolari, responsabili o persone designate/autorizzate al trattamento e se questi siano state adeguatamente istruiti sul trattamento	Eventuali Centri di Sperimentazione esterni partecipanti allo Studio, se previsti, in generale tratteranno i dati personali dei soggetti arruolati in qualità di autonomi Titolari ai sensi. dell'art.4, par.1, n. 7 del Regolamento UE 2016/679, ciascuno per gli ambiti di propria competenza come stabilito in apposite convenzioni o mediante sottoscrizione di specifici addendum contrattuali qualora coinvolti nello studio con un diverso ruolo privacy (Responsabile, Contitolare). Pertanto per poter effettuare lecitamente il trattamento dei dati relativi alle sperimentazioni, tali soggetti sono tenuti al rispetto delle disposizioni del Regolamento UE 2016/679 con particolare riferimento alle tipologie e alle modalità di trattamento dei dati, nonché alla custodia e sicurezza delle medesime informazioni predisponendo misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento e dalla natura dei dati da proteggere (art. 32 Regolamento UE 2016/679). Ulteriori soggetti terzi operanti per conto del Promotore o dei titolari degli altri centri partecipanti allo studio, se presenti, saranno nominati Responsabili del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/69 dai rispettivi Titolari.	**Accettabile**
Descrivere il flusso dati (cioè come i dati sono spostati o elaborati). Occorre descrivere il flusso analiticamente nei suoi vari passaggi, operazioni, attori	I dati clinici sono raccolti dopo che i pazienti sono stati sottoposti a trattamento o terapia, a partire dalle loro cartelle cliniche che, solitamente hanno come obiettivo quello di rispondere ad un quesito clinico che riguarda una strategia terapeutica, indagine clinica e/o attività di normale pratica clinica. Tali dati, in funzione della metodologia di conduzione dello studio saranno inseriti in maniera pseudonimizzata, secondo le modalità dettagliatamente specificato nel relativo Protocollo, su apposite piattaforme, fogli di calcolo Excel o altri strumenti software residenti sui Server aziendali o su singoli PC inseriti all'interno del dominio aziendale. In ogni caso l'accesso a tali risorse risulta adeguatamente controllato e protetto come descritto nella successiva sezione 2.4.	**Accettabile**
Indicare dove e come vengono archiviati i dati	Il processo analitico di raccolta, elaborazione e archiviazione dei dati oggetto dello studio è chiaramente documentato e illustrato nel corrispondente Protocollo.	**Accettabile**

Indicare sei dati sono trasferiti (si/no) ed eventualmente dove: (fuori dall'Azienda, fuori dall'Italia, fuori dall'Unione Europea)	Il trattamento dei dati dei pazienti partecipanti allo Studio generalmente non prevede il trasferimento al di fuori dell'ambito del Promotore o dell'Unione Europea. In ogni caso eventuali trasferimenti, con l'indicazione dei soggetti, dei luoghi in cui vengono trasferiti, sono dettagliatamente indicati nel Protocollo dello studio. Nel caso di trasferimento al di fuori della UE, come descritto nel Protocollo e nel successivo capitolo 2.4, verranno attivati i necessari meccanismi di garanzie di cui al capo V del Regolamento UE 679/2016.	**Accettabile**

2.3 PRINCIPI FONDAMENTALI – DIRITTI DEGLI INTERESSATI

PRINCIPI FONDAMENTALI		**Valutazione**
Limitazione delle finalità: indicare la base giuridica del trattamento, cioè la sua finalità lecita, quale prevista dal Regolamento UE 2016/679 (d'ora in poi Regolamento)	La base giuridica è rappresentata da: dati di natura comune: art. 6 par. 1 lettera e); dati particolari: art. 9 par. 2 lettera j), in combinato disposto con l'art. 89 GDRP e art. 110 comma 1 del D.Lgs. 196/2003, integrato con le modifiche introdotte dal D.Lgs. 101/2018 in adeguamento al Regolamento UE 69/2016 (GDPR), come successivamente novellato dall'art. 44, comma 1-bis della legge 29 aprile 2024, n. 56, di conversione del d.l. n. 19 del 2 marzo 2024 **(il consenso non è necessario).**	**Accettabile**
Minimizzazione dei dati: indicare i criteri utilizzati per garantire l'adeguatezza, la pertinenza e la non eccedenza dei dati utilizzati	I dati raccolti sono esclusivamente quelli indispensabili al raggiungimento degli obiettivi dello studio. I soggetti coinvolti a diverso titolo nella sperimentazione (es. medici, ricercatori, comitato etico di, autorità regolatorie), ciascuno per gli ambiti di propria competenza e in accordo alle responsabilità previste dalle norme della buona pratica clinica (d.l. 211/2003), tratteranno i dati personali dei pazienti inclusi nello studio, in particolare quelli sulla salute e, soltanto nella misura in cui sono indispensabili in relazione all'obiettivo dello studio, esclusivamente in funzione della realizzazione dello studio. I dati, trattati mediante strumenti anche elettronici, saranno diffusi solo in forma rigorosamente anonima, ad esempio attraverso pubblicazioni scientifiche, statistiche e convegni scientifici.	**Accettabile**
Limitazione della conservazione: indicare per quanto tempo sono conservati i dati e i criteri per la conservazione dei dati	I dati saranno conservati per un periodo di tempo non superiore a quello necessario agli scopi di ricerca per i quali sono stati utilizzati nel rispetto delle norme di legge che regolano la materia in oggetto e comunque per un periodo di almeno 7 anni, salvo diversa indicazioni contenute nel protocollo dello studio.	**Accettabile**
Esattezza dei dati: indicare le misure individuate per aggiornare, correggere o cancellare i dati che risultano non esatti in riferimento alla finalità per la quale sono trattati	I dati sono raccolti da medici esperti e competenti le cui capacità sono state valutate e ritenute idonee dal comitato etico di riferimento. La professionalità attestata delle persone coinvolte costituisce garanzia della corretta modalità di ottenimento dei dati necessari per la ricerca.	**Accettabile**

	I dati anagrafici, clinici e di laboratorio raccolti durante lo studio saranno identificati mediante un codice identificativo. Le informazioni raccolte per lo studio non saranno quindi indicate con l'anagrafica personale e solo il medico dello studio sarà in grado di associare il numero di identificazione ai diversi pazienti partecipanti alla ricerca. I dati verranno utilizzati esclusivamente a scopo di ricerca, in nessun modo i dati identificativi di un soggetto saranno utilizzati nelle pubblicazioni o relazioni scientifiche relative a questo studio. I risultati ottenuti dal presente studio saranno di proprietà degli sperimentatori, i quali tramite il PI, qualora espressamente indicato nel Protocollo, potranno eventualmente inserire in appropriati registri o altri strumenti pubblici di rilievo globale, quale ad esempio www.clinicaltrials.gov, un sommario del Protocollo prima dell'inizio dello Studio, ed il riepilogo dei risultati al termine dello stesso, entro i 12 (dodici) mesi successivi al completamento da parte di tutti i Centri; tale sommario dovrà includere il nome del Responsabile e degli altri sperimentatori coinvolti, nonché dei relativi ENTI; il PI si impegna altresì a tenere aggiornate queste informazioni per l'intera durata dello Studio.	
DIRITTI DEGLI INTERESSATI		**Valutazione**
Indicare come sono informati gli interessati al trattamento	Nell'impossibilità di contattare i singoli interessati verrà redatta, per ogni specifico studio, un'apposita informativa ai sensi degli artt. 13 e.14 del Regolamento e sarà pubblicata sul sito istituzionale del Promotore nell'apposita sezione "Informazioni per i pazienti studi retrospettivi" (https://www.ospedalideicolli.it/azienda/comitato-etico-2/). Nel caso di più centri partecipanti, il Promotore ha disposto che una analoga informativa sarà pubblicata anche sul sito istituzionale di ogni singolo centro partecipante allo studio in apposite sezioni facilmente accessibili.	**Accettabile**
Indicare come è acquisito il consenso degli interessati	Il consenso degli interessati non è richiesto in quanto lo studio prevede la raccolta dei dati personali in maniera retrospettiva. Ovvero, i dati sono già presenti nei sistemi del titolare del trattamento e raccolti in occasione delle prestazioni sanitarie precedentemente erogate. A tale riguardo poiché numerosi pazienti sono deceduti o risultati non reperibili, non essendo possibile informarli e raccogliere il relativo consenso si è fatto ricorso alle prescrizioni di cui all'art. 110 comma 1 del D.Lgs. 196/2003, integrato con le modifiche introdotte dal D.Lgs. 101/2018 in adeguamento al Regolamento UE 69/2016 (GDPR), nonché successivamente novellato dall'art. 44, comma 1-bis della legge 29 aprile 2024, n. 56, di conversione del d.l. n. 19 del 2 marzo 2024, anche nel rispetto di quanto previsto dall'art. 89 GDPR (**Il Consenso non è necessario**).	**Accettabile**

	A tale proposito, il titolare del trattamento (Promotore), nell'ottica di adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, tra cui acquisire il parere favorevole del competente comitato etico a livello territoriale sul protocollo di ricerca, dispone che nel protocollo di ricerca venga accuratamente motivata e documentata la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati e quindi acquisire il consenso, risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, se del caso documentando altresì i ragionevoli sforzi profusi per tentare di contattarli. Il protocollo di ricerca prevede, inoltre, che la suddetta disposizione venga estesa anche agli altri centri partecipanti allo studio, qualora previsti.	
Indicare come fanno gli interessati ad esercitare i loro diritti	L'interessato può esercitare il suo diritto secondo le indicazioni riportate nell'apposita "Procedura per la gestione dei diritti dell'interessato" pubblicata sul sito del Promotore all'indirizzo www.ospedalideicolli.it/privacy/, ovvero contattando il Titolare del trattamento o il DPO, come indicato nell' informativa relativa allo studio di competenza pubblicata nella sezione "Informazioni per i pazienti studi retrospettivi" (https://www.ospedalideicolli.it/azienda/comitato-etico-2/), informativa che, nel caso di studio multicentrico, riporterà anche i dati di contatto dei Titolari e dei DPO dei vari centri di sperimentazione partecipanti. Relativamente ai titolari dei dati dei soggetti arruolati allo studio dagli altri centri partecipanti (se previsti), nella relativa informativa, pubblicata sui propri siti istituzionali, oltre ai dati di contatto del proprio Titolare e Responsabile della Protezione dei dati (DPO), saranno indicati anche i dati di contatto del Titolare e del DPO del Promotore.	**Accettabile**
Valutare se, in caso di trasferimento dei dati al di fuori della UE, i dati godono di una protezione equivalente	Il trattamento dei dati dei pazienti partecipanti allo Studio generalmente non prevede il trasferimento al di fuori dell'Unione Europea. Un eventuale trasferimento, anche per finalità di farmacovigilanza (nel caso di studi osservazionali sul farmaco), prevedono esclusivamente comunicazioni (obbligatorie ai sensi dell'art. 5 comma 2 D.M. Salute 30 novembre 2021) di dati in forma pseudonimizzata. In tal caso, come descritto nel Protocollo dello studio, tali comunicazioni avverranno soltanto nel rispetto delle condizioni di cui agli artt. 44 e ss. di cui al capo V del Regolamento (UE). Eventuali ed ulteriori attività di trattamento che prevedono il trasferimento dei dati al di fuori della UE, nonché delle condizioni adottate per garantire un adeguato livello di protezione dei dati personali dei soggetti interessati, tra cui l'utilizzo delle Standard Contractual Clauses approvate dalla	**Accettabile**

	Commissione Europea con "Decisione di Esecuzione UE) 2021/914 della Commissione del 4 giugno 2021", sono anch'esse ampiamente indicate nel Protocollo dello studio.	

2.4 ANALISI MISURE TECNICHE ORGANIZZATIVE ADOTTATE

MISURE TECNICHE – ORGANIZZATIVE ADOTTATE		Valutazione
Formazione e formalizzazione del ruolo del personale addetto al trattamento dati	Sono predisposti appositi corsi di formazione per dipendenti e i collaboratori/fornitori in relazione alle responsabilità loro e dell'organizzazione relativamente alle tematiche di sicurezza delle informazioni e della protezione dei dati personali, incluso l'impegno a rispettare le norme ed i regolamenti vigenti (diritto d'autore, privacy, etc.), anche dopo la risoluzione o la modifica del loro stato occupazionale. Sono costantemente monitorate e gestite le attività di formazione relativamente a personale neo-assunto o a collaboratori temporanei (specializzandi, borsisti, tirocinanti, etc.), anche mediante la stabile disponibilità di un corso on line su piattaforma aziendale. Sono adottate e pubblicate sul sito aziendale procedure, linee guida e appositi format di atti di nomina per la formalizzazione dei ruoli di Delegato e Autorizzato al trattamento dati. (Modello atto di nomina a Delegato Interno, Modulo autorizzazione al trattamento dati). Una lista degli autorizzati (tutti coloro che a qualsiasi titolo trattano dati personali sotto l'autorità del Titolare) viene elaborata, aggiornata e conservata a cura dei responsabili delle UU.OO. della struttura di competenza.	**Accettabile**
Ove applicabile: indicare se gli obblighi del responsabile del trattamento sono chiaramente definiti e formalizzati, e in caso di risposta positiva precisare come	Ove presenti, gli obblighi dei responsabili del trattamento sono disciplinati con chiarezza in un apposito accordo per il trattamento dei dati personali (cfr. art. 28 del GDPR) secondo lo schema illustrato nella procedura "Nomina dei Responsabili Esterni" pubblicata sul sito aziendale https://www.ospedalideicolli.it/privacy/ contenente disposizioni per la corretta formalizzazione del ruolo ex. Art.28 GDPR e la giusta definizione degli obblighi tra le parti, individuando, per tutti i soggetti esterni che forniscono prodotti, servizi, attività o prestazioni, a qualsiasi titolo e che trattano dati per conto del Titolare, le diverse problematiche data protection.	**Accettabile**
Indicare le risorse tecniche organizzative a supporto del trattamento	In funzione della metodologia di conduzione dello studio e/o dalla disponibilità di eventuali strumenti messi a disposizione dai soggetti esterni, nonché delle indicazioni dettagliatamente specificate nel relativo Protocollo, i dati clinici dello studio, in ogni caso pseudonimizzati, potranno: • essere inseriti e trattati tramite uno specifico software, opportunamente specificato nel Protocollo, e memorizzati esclusivamente su un server centrale ospitato presso il CED e gestito dal responsabile del CED;	**Accettabile**

	• essere inseriti e trattati tramite uno specifico software, opportunamente specificato nel Protocollo, e memorizzati esclusivamente su un server cloud; • essere inseriti e trattati tramite uno specifico software, opportunamente specificato nel Protocollo, e memorizzati esclusivamente sulla PDL del PI ospitato presso la UO di competenza e gestito dal responsabile della UO; • possono essere inseriti e trattati tramite un foglio elettronico (Excel) e memorizzati esclusivamente sulla PDL del PI ospitato presso la UO di competenza e gestito dal responsabile della UO. In tutti i casi le risorse impiegate si trovano in aree riservate e presidiate per cui il loro accesso fisico risulta adeguatamente controllato. La protezione perimetrale dell'infrastruttura IT aziendale e il controllo degli accessi logici alle PDL risultano adeguate e vengono ampiamente descritte di seguito.	
Integrità e riservatezza dei dati: indicare le misure tecniche ed organizzative adottate per garantire la sicurezza dei dati rispetto a trattamenti non autorizzati o illeciti, perdita, distruzione o danni accidentali	La riservatezza dei dati è garantita dalla formazione e formalizzazione del ruolo di tutto il personale addetto al trattamento dati. La integrità e disponibilità dei dati sono garantite dalle misure tecniche adottate a protezione della infrastruttura IT aziendale.	**Accettabile**
Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono pseudonimizzati, e secondo quali modalità	Le modalità di pseudonimizzazione dei dati avverranno attraverso l'assegnazione di un codice numerico/alfanumerico (Subject ID). I dati personali sono trattati in associazione con questa informazione non direttamente identificativa, e la correlazione tra questa e i dati identificativi dell'interessato è conservata separatamente, accessibile al solo personale coinvolto nello studio, assicurandone, con idonee misure di sicurezza tecniche ed organizzative, la riservatezza. Il Subject ID consisterà in un codice numerico/alfanumerico, generato ogni qual volta un nuovo paziente viene arruolato nello studio.	**Accettabile**
Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono crittografati, e secondo quali modalità	Qualora è previsto l'inserimento dei dati su un'apposita piattaforma, l'accesso e il trasferimento dei dati da e verso tale piattaforma avvengono tramite protocollo https con le modalità descritte nel sempre protocollo. Ulteriori dettagli sulle modalità di inserimento e trasferimento sono di seguito riportati, oltre che dettagliatamente specificati nel Protocollo.	**Accettabile**
Indicare se esiste una piattaforma per la gestione della sperimentazione e con quali misure e cautele viene effettuato il trasferimento/inserimento dei dati o,	Qualora venga utilizzata una piattaforma per la gestione dello studio, i dati una volta inseriti sulla piattaforma vengono cancellati da ogni altra fonte. Nel caso invece la gestione dello studio avvenga tramiti l'utilizzo di file Excel questi, oltre alle misure di controllo di accesso alle PDL di seguito descritte,	**Accettabile**

nel caso contrario, quali misure e cautele vengono utilizzate per proteggere i file contente i dati dello studio	sono ulteriormente e adeguatamente protetti da password conformemente custodite e protette.	
Indicare se nel trattamento o in qualche sua fase (specificare) i dati sono anonimizzati, e secondo quali modalità	I dati sono assolutamente anonimizzati prima della pubblicazione.	**Accettabile**
Indicare i criteri di profilazione per l'accesso ai dati	L'accesso ai dati è consentito ai soggetti coinvolti a diverso titolo nella sperimentazione (es. medici, ricercatori, monitor, data manager, personale sanitario, comitato etico,), ciascuno per gli ambiti di propria competenza e responsabilità.	**Accettabile**
Specificare come il protocollo dello studio è integrato nel progetto privacy aziendale	L'Azienda, conformemente alla disciplina del Reg. (UE) 2016/679, gestisce i dati nel rispetto del principio di privacy by design e by default. La gestione di informativa e consenso e la modalità di utilizzo dei dati è stata pensata sempre tenendo in considerazione la protezione dei dati dei pazienti I principi fondamentali, le modalità per garantire i diritti degli interessati, le misure tecniche ed organizzative adottate sono espressamente indicate all'interno di ciascun Protocollo da sottoporre al Comitato Etico per l'approvazione, secondo le specifiche fornite dal U.O.C P.T.I..	**Accettabile**
Indicare le misure per il controllo accesso alle postazioni di lavoro	Il controllo dell'accesso alle PDL è garantito nell'ambito di un dominio attraverso Microsoft Active Directory (AD) che gestisce le richieste di autenticazione per la sicurezza (login, controllo dei permessi, ecc.), tramite il servizio MFA (Multi Factor Authentication), anche per accessi alla posta elettronica. Il servizio MFA garantisce anche il controllo della validità delle credenziali di accesso.	**Accettabile**
Indicare se gli accessi sono tracciati	Gli accessi ai pc di dominio sono tracciati direttamente da Active Directory, quelli relativi alle PDL non in dominio sono gestiti localmente sulle PDL mentre quelli delle risorse in rete vengono gestiti da Active Directory centrale.	**Accettabile**
Indicare le misure di sicurezza dei siti web	Generalmente non sono utilizzati siti web nel trattamento dei dati dello studio. In ogni caso il filtro degli accessi ai canali web è gestito attraverso il firewall dal servizio content filtering, oltre che dal servizio antispam di Microsoft 365.	**Accettabile**
Indicare le misure adottate per la sicurezza dei canali informatici	I canali informatici di collegamento tra eventuali ulteriori soggetti coinvolti nello studio sono protetti da Firewall e sistemi di rilevamento delle intrusioni che monitoreranno e filtreranno l'accesso ai dati, proteggendo la rete da attacchi esterni. L'accesso ai dati è consentito mediante un sistema di autenticazione MFA unicamente a persone formate ed autorizzate. La trasmissione e comunicazione dei dati, ove prevista, avviene con l'utilizzo di protocolli SSL E HTTPS.	**Accettabile**
Indicare con quale frequenza e in che modo viene effettuato il backup dei	Il backup dei dati, come specificato nel Protocollo dello studio, viene effettuato regolarmente. Nel Protocollo sono	**Accettabile**

dati	descritte anche le modalità con cui esso viene effettuato a seconda delle risorse tecniche utilizzate a supporto del trattamento (computer locali, server, cloud, etc.) e degli strumenti software impiegati (piattaforma web, programma software dedicato, file locali (Access, Excel), etc.).	
Indicare se il sistema prevede misure contro virus e malware	Per tutte le PDL è' attivato il servizio ANTIVIRUS SOPHOS MDR che garantisce un livello di protezione molto elevato perché consente attività di monitoraggio su tutte le attività svolte dal client; è dotato anche di un agent che interviene in maniera tempestiva quando si verificano cambiamenti nei file, bloccando immediatamente l'operazione in corso, e contattando i referenti aziendali per un diretto intervento operativo.	**Accettabile**
Indicare se i dati sono trattati anche su supporti cartacei, e come questi sono gestiti	I documenti afferenti la sperimentazione sono conservati per un periodo di almeno 7 anni dalla chiusura dello studio, salvo diversa indicazione contenuta nel protocollo, in contenitori sigillati, all'interno dei locali della UO di svolgimento dello studio con accesso limitato.	**Accettabile**
Indicare le misure per il controllo degli accessi fisici	Tutti i PC/servers si trovano in aree riservate e presidiate.	**Accettabile**
Descrivere i processi per la gestione di eventuali Data Breach	E' stata predisposta e divulgata al personale una procedura relativa alla gestione degli eventi di sicurezza e/o incidenti di sicurezza formalizzata con ruoli prestabiliti. E' stata istituita una casella di posta elettronica dedicata alle eventuali segnalazioni. Viene redatto e mantenuto un registro degli eventi di violazione o presunta violazione che contenga almeno informazioni sulla scoperta, l'analisi, il contenimento, la mitigazione e il recupero dai vari incidenti di sicurezza.	**Accettabile**

3 VALUTAZIONE DEL RISCHIO

L'obiettivo della valutazione dei rischi è di stimare il livello di "**rischio effettivo**" per i diritti e le libertà dell'interessato connesso al trattamento in esame con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento.

Il livello di rischio effettivo è inteso come la probabilità che una minaccia possa sfruttare le vulnerabilità di un asset o di un gruppo di asset a supporto del trattamento e quindi causare un danno all'interessato.

Di seguito il livello di rischio effettivo viene stimato in termini di:

- "Impatto potenziale (**I**)" sull'interessato nel caso in cui si concretizzi ognuno degli scenari di rischio sotto indicati;
- "Probabilità di accadimento delle minacce (**P**)", dipendente principalmente dal livello di vulnerabilità delle misure adottate a supporto delle minacce e dalla capacità delle stesse di sfruttarle.

Gli scenari di rischio presi in considerazione nel definire la stima della valutazione in oggetto sono:

- Perdita di riservatezza - accesso illegittimo ai dati personali;
- Perdita di integrità - modifica non autorizzata dei dati personali;
- Perdita di disponibilità - perdita, furto, cancellazione non autorizzata di dati personali.

3.1 ANALISI DEGLI IMPATTI SULL'INTERESSATO

Il rischio che possa verificarsi l'accadimento di qualche minaccia può comportare una violazione dei diritti e le libertà dell'interessato provocandogli danni fisici, materiali e psicologici (impatto).
Ciò richiede la necessità di definire un criterio per la valutazione dell'impatto di tali danni sugli interessati. Nello specifico, per ognuno degli scenari di rischio sopra definiti, è stata condotta l'analisi degli impatti potenziali sui diritti e le libertà dell'interessato in termini:

- Categoria di impatto fisico (danno fisico);
- Categoria di impatto materiale (danno materiale);
- Categoria di impatto psicologico (danno psicologico)

Tenendo conto della specificità e delle caratteristiche dei dati trattati (*i dati oggetto dello studio sono già presenti nei sistemi del titolare del trattamento perché raccolti in occasione delle prestazioni sanitarie precedentemente erogate…..*) e sulla base delle pratiche più diffuse per le problematiche di gestione dei rischi e su indicazioni di best practicies per il settore sanitario, indipendentemente dalla categoria è stato valutato un livello di impatto, espresso secondo una scala di valutazione qualitativa discreta (N.A.= Non Applicabile, 1=Trascurabile, 2=Limitato, 3=Significativo, 4=Massimo) come di seguito riportato (**2=Limitato)**.

	Perdita di Riservatezza *Accesso illegittimo ai dati personali*	**Perdita di Integrità** *Modifica non autorizzata dei dati personali*	**Perdita di Disponibilità** *Perdita, furto, cancellazione non autorizzata di dati personali*
Massimo impatto calcolato su tutte le categorie	**2**	**2**	**2**

Tabella Livello di Impatto complessivo per scenario

Legenda:

1	Trascurabile
2	Limitato
3	Significativo
4	Massimo

3.2 VALUTAZIONE DELLA PROBABILITÀ DI ACCADIMENTO DELLE MINACCE

Sulla base di standard e best practices internazionali di sicurezza e privacy e del documento ENISA "*Manuale sulla Sicurezza nel trattamento dei dati*", anche la probabilità di accadimento di una minaccia è stata espressa su una scala di valutazione qualitativa di 4 livelli (**Trascurabile, Limitata, Significativa, Massima**) con riferimento ai tre scenari di rischio relativi alla perdita di **riservatezza, integrità e disponibilità**.

Per ogni scenario di rischio, come già più volte specificato, la probabilità di accadimento delle corrispondenti minacce è stata definita seconda una relazione inversa al livello di attuazione e di efficienza delle diverse misure predisposte per contrastarle, ovvero delle misure poste in essere a protezione del trattamento in esame (una singola minaccia generalmente prevede anche più misure di contrasto).

A tale riguardo il valore qualitativo del livello di implementazione e di efficienza di ogni singola misura, come riportato ai par. 2.3 e 2.4, è stato classificato secondo la seguente scala:

- **NA (Non Applicabile):** misura non applicabile perché non richiesta o non pertinente;

- **Assente (Non Applicata):** misura richiesta ma inesistente o totalmente inefficiente;
- **Parziale (Applicata Parzialmente):** misura insufficiente, di basso livello di efficienza;
- **Accettabile (Sufficiente):** misura applicata di livello accettabile;
- **Totale (Totalmente Adeguata):** misura totalmente applicata di livello adeguato.

La corrispondenza tra tale valore di efficienza globale delle misure adottate e la probabilità di accadimento della minaccia da contrastare viene determinata secondo la relazione seguente:

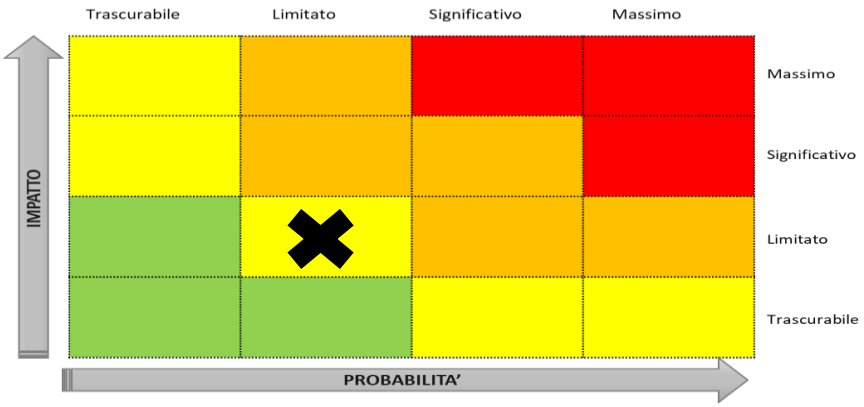
Peso Efficienza Misure Adottate	*Probabilità Accadimento Minaccia*
Totale	**Trascurabile**
Accettabile	**Limitato**
Parziale	**Significativo**
Assente	**Massimo**

Sulla base della suddetta relazione, Il livello **"Accettabile"** di efficienza delle misure tecniche-organizzative dettagliatamente riscontrato e riportato nei paragrafi precedenti (par. 2.3 e 2.4), per ogni scenario di rischio ha determinato, secondo la suddetta relazione, un livello di probabilità di accadimento delle minacce come riportato nella tabella seguente.

SCENARIO DI RISCHIO-MINACCIA	*PROBABILITA' ACCADIMENTO MINACCIA*
ACCESSO ILLEGITTIMO AI DATI (RISERVATEZZA)	**Limitato**
MODIFICHE INDESIDERATE DEI DATI (INTEGRITA')	**Limitato**
PERDITA DEI DATI (DISPONIBILITA')	**Limitato**

3.3 VALUTAZIONE DEL RISCHIO EFFETTIVO

Secondo le indicazioni riportate nella Norma DS/ISO/IEC 29134:2017 (Annex A) e nel documento ENISA "*Manuale sulla Sicurezza nel trattamento dei dati*", il **Rischio Effettivo** per i diritti e le libertà degli interessati, nel caso di accadimento della minaccia, si ottiene combinando la probabilità di accadimento della minaccia (par. 3.2) con il massimo livello di impatto (par. 3.1). Nello specifico, la corrispondenza fra la gravità (**I**) di un rischio (impatto potenziale sugli interessati) e la probabilità di accadimento **(P)** dell'evento minaccia che provoca il danno: **R = f(P, I),** è definita dalla seguente relazione.



Correlazione Indice Gravità Impatto - Probabilità Accadimento Minacce

Combinando secondo la relazione sopra illustrata i singoli scenari di minaccia (par. 3.2) con il livello di impatto massimo di valore **"Limitato" (**par. 3.1), per ognuno degli scenari di rischio di riferimento è stato riscontrato un valore di **Rischio Effettivo** per i diritti e le libertà degli interessati come di seguito riportato.

SCENARIO DI RISCHIO-MINACCIA	*LIVELLO DI RISCHIO EFFETTIVO*
ACCESSO ILLEGITTIMO AI DATI (RISERVATEZZA)	**Limitato**
MODIFICHE INDESIDERATE DEI DATI (INTEGRITA')	**Limitato**
PERDITA DEI DATI (DISPONIBILITA')	**Limitato**

Legenda:

1	Trascurabile
2	Limitato
3	Significativo
4	Massimo

4 EXECUTIVE SUMMARY

Relativamente al trattamento in esame, la Data Protection Impact Assessment ha evidenziato che il massimo valore di **Rischio Effettivo** per i diritti e le libertà degli interessati risulta essere di valore **"Limitato"** indipendentemente dallo scenario di rischio di riferimento (**riservatezza, integrità e disponibilità**), in base al quale occorre definire la **eventuale strategia di trattamento del rischio da adottare.**

A tale proposito, convenuto che tale valore è ritenuto accettabile dal Titolare, si CONCLUDE che non è richiesta alcuna "Strategia del Trattamento del Rischio" né, tantomeno, la necessità di attuare un "Piano di Azione/Sicurezza" per la definizione di interventi volti alla riduzione del suddetto livello di rischio.