VALUTAZIONE D'IMPATTO PER PROGETTI DI RICERCA IN AMBITO SANITARIO

SU DATI RETROSPETTIVI

(ART. 110 D. LGS. 196/2003, Provvedimento Garante n. 146/2009)

La valutazione di impatto (DPIA) consente di identificare in modo puntuale i rischi per la protezione dei dati personali quando vengono pianificati nuovi progetti di ricerca o aggiornati progetti di ricerca in corso e di individuare le azioni necessarie per mitigare tali rischi.

Una valutazione di impatto, secondo l'Autorità Garante per la protezione dei dati personali, deve sempre essere effettuata negli studi retrospettivi quando:

- il trattamento dei dati personali è su larga scala;
- vengono trattate categorie particolari di dati, ad esempio dati genetici;
- l'attività comporta il data linkage di molteplici e diversi archivi di dati;
- l'attività prevede la rilevazione di dati per individui vulnerabili (minori, soggetti con patologie psichiatriche, anziani, ecc.);
- la base giuridica per il trattamento dei dati non è riferibile al consenso al trattamento, a ricerche condotte sulla base di disposizioni di legge o regolamento o al diritto, o ad altre specifiche fattispecie previste dal GDPR e dal Codice Privacy.

Titolo dello studio: Valutazione clinica e della qualità di vita dei pazienti affetti da malattie cutanee infiammatorie in trattamento con farmaci a bersaglio molecolare

Codice di Protocollo: Derm-Care

Titolare del trattamento: Università degli Studi di Modena e Reggio Emilia (UNIMORE) e per essa il Dipartimento di CHIMOMO, in qualità di Promotore dello studio.

Struttura/Dipartimento/U.O./Servizio Le entità coinvolte, ciascuna da qualificarsi quale autonomo titolare del trattamento, sono le seguenti:

- *Centro Promotore*: Università degli Studi di Modena e Reggio Emilia, Dipartimento di CHIMOMO,
- *Centro Sperimentatore*: SC DERMATOLOGIA AOU DI MODENA.

Soggetto delegato: P.I. dello Studio è PROF. MARCO MANFREDINI.

Data compilazione: 25 NOVEMBRE 2025

TRATTAMENTO DEI DATI
Descrizione del trattamento *(compilare i campi successivi e allegare il modulo di fattibilità dello studio)*

Obiettivi dello studio	Valutare la variazione dell'indice DLQI indotta dalle terapie a bersaglio molecolare, in una coorte di pazienti affetti da malattie infiammatorie croniche cutanee.
Breve sintesi del progetto	Si tratta di uno studio osservazionale retrospettivo descrittivo, monocentrico e non interventistico, con cartelle cliniche ospedaliere come fonte dei dati. **L'OBBIETTIVO è** valutare la variazione dell'indice DLQI indotta dalle terapie a bersaglio molecolare, in una coorte di pazienti affetti da malattie infiammatorie croniche cutanee. Saranno arruolati Soggetti di età compresa tra i 1 e i 100 anni, maschi o femmine, che abbiano iniziato una delle seguenti terapie a bersaglio molecolare, nel periodo di studio (1/1/2020 al 1/8/2025):Adalimumab, Certolizumab pegol,Secukinumab,Ixekizumab,Brodalumab,Bimekizumab,Ustekinumab,Risankizumab,Tildrakizumab, Guselkumab,Deucravacitinib,Upadacitinib,AbrocitinibBaricitinib,Ritlecitinib. Saranno arruolati tutti i pazienti idonei che daranno il loro consenso informato per un massimo di 80 pazienti. ~~Tuttavia, lo sperimentatore non ha certezza di poter raggiungere tutti i pazienti per raccogliere consenso informato e consenso al trattamento dei dati personali~~. Lo studio avrà durata di 10 mesi.
Tipologia di dati raccolti	
Modalità di raccolta *(barrare anche più caselle)*	☒ consultazione cartelle cliniche/documentazione sanitaria ☐ archivi di dati clinici ☐ archivi di test diagnostici ☐ dati di laboratorio ☐ altro (specificare) _____
Trattamento dei dati *(indicare il supporto utilizzato per la rilevazione e conservazione dei dati)*	☒ In formato cartaceo ☒ In formato digitale ☐ altro (specificare) _____ Si specifica che verranno consultate cartelle cliniche/documentazione sanitaria in cartaceo presso il centro sperimentatore. Tuttavia, saranno estratti dati personali trattati successivamente in formato digitale.
Categorie di persone interessate	☒ Pazienti ☐ Persone sane ☐ operatori sanitari ☒ soggetti vulnerabili ☐ altro (specificare) _____

Categorie di dati trattati	☒ dati sulla salute fisica o psichica ☐ dati genetici ☐ informazioni sulla vita sessuale ☐ informazioni sull'orientamento sessuale ☐ informazioni sugli stili di vita e le condizioni socioeconomiche ☐ informazioni su istruzione e formazione professionale ☐ anamnesi lavorativa ☐ informazioni su religione o altre credenze ☐ *altro (specificare)* _____
I dati personali vengono comunicati /condivisi con altri?	☐ No ☒ Sì Se sì, selezionare uno o più ambiti di comunicazione e la natura dei dati comunicati: ☒ Promotori ☐ Dati in chiaro ☒ Dati pseudonimizzati ☐ Dati anonimi/anonimizzati ☐ altro (specificare) I dati raccolti presso il centro sperimentatore sono condivisi esclusivamente con il Promotore secondo le modalità descritte nel presente DPIA. ☐ CRO ☐ Dati in chiaro ☐ Dati pseudonimizzati ☐ Dati anonimi/anonimizzati ☐ altro (specificare) ☐ altro (specificare) _____ ☐ Dati in chiaro ☐ Dati pseudonimizzati ☐ Dati anonimi/anonimizzati ☐ altro (specificare)
I dati personali vengono trasferiti all'estero?	☒ No ☐ Sì Se sì, qual è la natura dei dati trasferiti: ☐ Dati in chiaro ☐ Dati pseudonimizzati ☐ Dati anonimi/anonimizzati ☐ altro (specificare) Se sì, ☐ Paesi area UE ☐ Paesi extra UE

	In quale/i Paese/i all'interno dell'area o extra UE _____
Misure di protezione dei dati	
Verranno conservati i dati identificativi dei partecipanti?	☒ No ☐ Sì Se sì, specificare le ragioni sottese a tale esigenza: _____.
Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca	Per non identificare direttamente l'interessato sono adottate le seguenti misure: ☐ Adozione di tecniche crittografiche ☒ Utilizzo di codici univoci per ciascun partecipante. Solo il responsabile della ricerca può (con l'uso di mezzi ragionevoli) collegare i codici all'identità dei partecipanti ☐ Altro, specificare in dettaglio _____ _____ Per anonimizzare o aggregare i dati, anche in un momento successivo alla raccolta, sono adottate le seguenti misure: ☐ I dati personali, a seguito della raccolta sono eliminati definitivamente senza la possibilità di risalire ai dati originali ☐ I dati personali sono sostituti da uno o più identificatori, che possono essere utilizzati per un set di dati o per ogni singolo dato con distruzione del dato personale originario ☒ Al termine della ricerca sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati ☐ Altro (specificare) _____ _____

PRINCIPI, FINALITA' E BASI GIURIDICHE	
Necessità e proporzionalità	
Sono trattati solo i dati necessari e pertinenti al perseguimento delle finalità della ricerca (Minimizzazione)?	☒ Sì ☐ No Se no, specificare i motivi e le azioni previste _____ _____ _____

Integrità ed esattezza	
Sono state messe in campo azioni per garantire l'integrità ed esattezza dei dati?	☒ Sì ☐ No Se no, specificare i motivi e le azioni previste _____ _____
Limitazione della conservazione	
Per quanto tempo verranno conservati i dati raccolti?	Indicare il numero di mesi/anni: 7 ANNI DALLA FINE DELLO STUDIO Decorso tale termine i dati che rimarranno come patrimonio della ricerca saranno, dunque: ☐ Anonimizzati completamente ☐ Distrutti ☒ altro (*specificare*) Sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati.
Basi giuridiche	
Quali sono le basi giuridiche del trattamento?	☐ art. 9, par. 2, lett. j) GDPR[1] ☐ art. 110, co. 1 primo periodo Codice Privacy[2] ☒ art. 110, co. 1, secondo periodo Codice Privacy[3] ☐ art. 110 bis, co. 4: Istituto di Ricerca e Cura a carattere scientifico per le attività di assistenza e ricerca dell'ambito di riconoscimento[4]

MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO

Informativa e consenso

[1] il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

[2] Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a 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, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento.

[3] Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

[4] Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e 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 Regolamento. *[ndr: Eccezione prevista per gli IRCCS con riferimento al trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici, per il quale i titolari non IRCCS devono effettuare la DPIA e richiedere il parere del Garante]*

SOLO SE LA BASE GIURIDICA È L'ART. 110, CO. 1, SECONDO PERIODO ***Indicare i motivi per i quali non è possibile fornire l'informativa ai partecipanti allo Studio (soggetti interessati) e acquisirne il consenso***	☐ motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione ☒ sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati in ragione: ☐ del numero molto alto di interessati che è stato stimato ☒ del fatto che gli interessati sono deceduti o non contattabili Come si rappresentava nella sezione "***Breve sintesi del progetto***" seppur la procedura che si intende adottare prevede un contatto con il paziente e una raccolta del consenso informato e del consenso al trattamento dei dati, non si può escludere che alcuni pazienti siano irraggiungibili o deceduti.
Nel caso di studi retrospettivi su dati genetici, ove non sia possibile ottenere il consenso informato, indicare se ricorrono le condizioni indicate	☐ indagini statistiche o ricerche scientifiche previste dal diritto dell'Unione europea, dalla legge o, nei casi previsti dalla legge, da regolamento ☐ scopi scientifici e statistici direttamente collegati con quelli per i quali è stato originariamente acquisito il consenso informato degli interessati ☒ sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati e il programma di ricerca comporta l'utilizzo di campioni biologici e di dati genetici che in origine non consentono di identificare gli interessati, ovvero che, a seguito di trattamento, non consentono di identificare i medesimi interessati e non risulta che questi ultimi abbiano in precedenza fornito indicazioni contrarie
Esercizio da parte dell'interessato dei diritti ex artt.15-22 DPR	
È stata predisposta una procedura ad hoc da parte dell'Ente?	☒ Sì ☐ No

A CURA DELL'UNIVERSITÀ

È opportuno premettere che in tale sezione sono riportate le misure tecniche ed organizzative garantite da Unimore. In un'ottica di progetto tali misure andranno certamente integrate con quelle del Centro Partecipante.

Si ricorda, infatti, che i dati personali sono trattati in chiaro esclusivamente presso il Centro Partecipante e vengono trasmessi al Promotore in forma pseudonimizzata. Focalizzando l'attenzione esclusivamente sui sistemi Unimore, non sussiste alcuna possibilità di risalire all'identità dei soggetti interessati.

È dunque necessario considerare che per tutti i trattamenti realizzati presso il Centro Partecipante rilevano i mezzi e le relative misure di sicurezza dallo stesso adottate.

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO		
MISURA	Esistenti	Note
Organigramma interno	X	Predisposto con regolamento interno.
Nomine responsabili esterni	X	Nello studio di specie non sono predisposte, tuttavia l'università è dotata di template.
Nomina DPO	X	Contratto Rep. nr. 10/2025 e Atto di designazione del 16.7.2025 - prot. nr. 211401 - rep. nr. 726/2025

Informativa	X	Ordinariamente il titolare predispone informative per i trattamenti realizzati. Nel caso di specie, la procedura che si intende adottare prevede un contatto con il paziente per la raccolta del consenso informato e del consenso al trattamento dei dati. Tuttavia, non si può escludere che alcuni pazienti siano irraggiungibili o deceduti, pertanto a tali pazienti non verrà sottoposta alcuna informativa.
Istruzioni persone autorizzate trattamento	X	Il personale coinvolto riceve adeguate istruzioni in sede di incarico al trattamento e mediante le policy adottate e circolarizzate dal titolare.
Formazione	X	Il personale coinvolto è sensibilizzato e formato in materia di data protection.
Registri	X	Il titolare ha predisposto i registri dei trattamenti realizzati ai sensi dell'art. 30 GDPR e delle Linee guida CODAU.
Procedure	X	Il Titolare ha adottato le necessarie procedure per garantire un'adeguata *compliance* GDPR.
Politiche di tutela della privacy	X	L'attività del titolare è orientata ad una strutturata *compliance* GDPR: > designato DPO esterno con il quale intercorre uno stretto confronto; > adottate misure tecniche ed organizzative; > implementate misure tecniche di sicurezza ICT richieste da AGID; > adottati regolamenti e procedure interni in materia di *data protection;*
Distruzione/smaltimento sicuro cartaceo	X	Non applicabile nel caso di specie. Si ribadisce che la documentazione cartacea viene in rilievo solo nella prima parte dell'attività di estrazione di dati. Si tratta di cartelle cliniche/documentazione sanitaria del Centro sperimentatore che non vengono in nessun modo successivamente coinvolte nelle attività dello Studio (pertanto non devono essere distrutte o smaltite dal Promotore).
Inventario degli asset	X	• Inventario dei dispositivi autorizzati e non autorizzati: Sono gestiti attivamente tutti i dispositivi *hardware* sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia permesso solo ai dispositivi autorizzati e che i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso. Sono adottate misure per ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni, portatili, periferiche, dispositivi, supporti removibili ecc.) siano utilizzate per danneggiare dati personali. • Inventario dei software autorizzati e non autorizzati: Sono gestiti attivamente tutti i *software* sulla rete in modo che sia installato ed eseguito solo il software autorizzato, mentre il *software* non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione. Sono adottate misure per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni, *software* ecc.) vengano sfruttate per danneggiare i dati personali trattati. Si tratta di: aggiornamenti, protezione fisica e accessi, lavoro su spazio di rete protetto, controlli di integrità, *logging* ecc.
Misure anti – intrusive (cartelli di divieto di accesso ai locali, strumenti per la rilevazione degli accessi, guardiania, portineria, serrature armadi, schedari, ecc.)	X	• Sono adottate misure per il controllo degli accessi fisici agli uffici universitari, nonché ai "locali strategici" (es. locali server, locali pc, archivi). • Sono implementati sistemi di protezione adeguati volti a garantire la sicurezza della rete (es. *firewall* e *antivirus*).

Politiche di sicurezza informatica	X	• Istituita, implementata e gestita attivamente (tracciata, segnalata, corretta) la configurazione di sicurezza di *laptop*, *server* e *workstation* utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni. • Acquisite, valutate e intraprese continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.
Controllo accessi (log)	X	• Sono adottati Regolamenti e Procedure per la gestione degli incarichi al trattamento del personale, nonché delle relative credenziali di accesso ai sistemi/file autorizzati. • Sono adottate regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.
Antivirus / firewall	X	• Sono implementati sistemi di protezione adeguati volti a garantire la sicurezza della rete (es. *firewall* e *antivirus*). • Sono adottate misure volte a proteggere l'accesso alla rete, le postazioni ed i server contro malware che potrebbero compromettere la sicurezza dei dati personali trattati.
Politiche di clear screen	X	Non applicabile al caso di specie.
Back – up dei dati	X	• L'università adotta politiche di *backup* tali da assicurare la disponibilità e l'integrità dei dati personali. • Come richiesto da AGID, sono adottate procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.
Politiche di trasmissione dei dati	X	I dati non vengono trasmessi dal Promotore ad altre parti terze. Per quanto attiene alla trasmissione dati Centro Sperimentatore – Promotore si applica quanto previsto dal Modulo trasmissione dati.
nel caso si utilizzi un sito web esterno:		Non applicabile nel caso di specie.
Connessione sicura		
Accesso protetto da utenza personale		
Crittografia		Non applicata nel caso di specie.
Anonimizzazione	X	Misura applicata al termine del periodo di ricerca: il file contenente le chiavi di decodifica viene definitivamente e irreversibilmente cancellato, rendendo il data set oggetto dello studio completamente anonimizzato.
Pseudonimizzazione	X	Dopo l'estrazione dei dati, ogni attività di analisi e studio viene effettuata su un'estrazione pseudonimizzata. Si tratta di attività nelle quali i dati non possono più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive. Queste ultime sono conservate separatamente in un file ad accesso riservato al solo PI
Sicurezza dei documenti cartacei		Non applicabile nel caso di specie
Gestione postazioni	X	Le postazioni sono accessibili ai soli utenti universitari. È adottato un regolamento sul corretto utilizzo delle postazioni informatiche
Autenticazione	X	Sono creati, affidati e gestisti diversi profili utente in virtù delle mansioni svolte. In particolare, ogni utente dei sistemi del titolare è dotato di un User e di una password creata nel rispetto dei regolamenti interni.

Policy di gestione data breach	X	• Sono adottate adeguate procedure di gestione dei data breach; • In via preventiva sono acquisite, valutate e intraprese continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.
Minimizzazione	X	Il processo di trattamento dei dati effettuato nel progetto è tarato sui soli dati considerati necessari al raggiungimento degli obiettivi della ricerca. Ciò in considerazione: • della selezione "*by design*" a monte dei soli dati effettivamente pertinenti ed adeguati al raggiungimento delle finalità del progetto. • della limitazione dell'accesso ai dati; • della realizzazione delle attività di ricerca su un data set pseudonimizzato.

APPENDICE

Alla luce di quanto specificato in premessa al prospetto "*Misure di sicurezza applicate al trattamento*", la valutazione di impatto di seguito operata prende le mosse dalle misure adottate ordinariamente da UNIMORE con riferimento agli Studi Clinici (parificabili a quello di specie) nei quali i dati personali siano trattati nei sistemi universitari. Pertanto, tale valutazione è suscettibile di integrazione e deve necessariamente tenere in considerazione anche le specifiche misure di sicurezza adottate dall'AOU con riferimento ai propri sistemi.

APPENDICE

MINACCE
ACCESSO ILLEGITTIMO AI DATI
Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare? Perdita di riservatezza dei dati personali coperti da segreto professionale; perdita del controllo dei propri dati; decifratura non autorizzata dei dati pseudonimizzati; diffusione dei dati non autorizzata. **Quali sono le principali minacce che potrebbero concretizzare il rischio?** Utilizzo inappropriato delle password di accesso ai pc universitari e al database di raccolta dati; sottrazione delle password di accesso da parte di un terzo; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; accesso non autorizzato all'archivio delle cartelle cliniche dei pazienti arruolati nello studio; virus. **Quali sono le fonti di rischio?** Fonti umane interne (lasciare incustodita la postazione di lavoro, lasciare incustodite sulla scrivania eventuale documentazione che riporta dati personali dei pazienti arruolati nello studio, errore di integrazione applicativa). Fonti umane esterne (hacker).

Fonti non umane (virus, applicativi che interoperano con il SW, introduzione di bug in seguito ad aggiornamento dell'applicativo)

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); Antivirus/firewall; Politiche di trasmissione dei dati; Anonimizzazione; Pseudonimizzazione.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

La gravità del rischio è **Bassa**. L'impatto sugli interessati potrebbe essere oggettivamente elevato, considerando la natura e la quantità di dati trattati nello studio, tuttavia le misure previste per evitare gli accessi non autorizzati rendono estremamente limitata la probabilità di accadimento.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

La probabilità di concretizzazione del rischio è **Molto bassa**. Come descritto nel presente DPIA, le attività del progetto sono realizzate tramite l'utilizzo di codici univoci per ciascun partecipante. Solo il responsabile della ricerca (PI del progetto), può collegare i codici all'identità dei partecipanti: un soggetto terzo che accede al solo file pseudonimizzato senza avere il codice univico avrà a disposizione solo un elenco di informazioni non riferibili a persone fisiche identificate o identificabili. Non si integrerebbe, dunque, un accesso illegittimo a dati personali. Anche in eventuali scenari più complessi (quali, ad esempio, l'accesso illegittimo al data set pseudonimizzato e al file con le chiavi decodifica), la probabilità del rischio è comunque trascurabile. Ciò in virtù del fatto che:
a tutela degli ambienti e dei sistemi universitari in cui sono conservati il data set e il file con le chiavi di decodifica sono adottate tutte le misure di sicurezza ICT considerate minime e necessarie dall'AGID. Tali misure sono periodicamente aggiornate in linea con il progresso tecnologico.

MODIFICHE INDESIDERATE DEI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Perdita di integrità del dato con conseguente alterazione della qualità e affidabilità dell'attività di ricerca e degli esiti dello studio per il miglioramento delle conoscenze scientifiche e degli interventi di medicina preventiva.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Utilizzo inappropriato delle password di accesso ai pc universitari e al relativo database di raccolta dati; sottrazione delle password di accesso da parte di un terzo; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; accesso non autorizzato all'archivio delle cartelle cliniche dei pazienti arruolati nello studio; virus.

Quali sono le fonti di rischio?

Fonti umane interne (lasciare incustodita la postazione di lavoro, lasciare incustodite sulla scrivania eventuale documentazione che riporta dati personali dei pazienti arruolati nello studio, alterazione volontaria di dati, errore umano involontario).

Fonti umane esterne (hacker).

Fonti non umane (virus, applicativi che interoperano con il SW)

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

La misura più significativa è la limitazione dell'accesso ai file contenenti i dati pertinenti allo studio esclusivamente al PI, mediante i dispositivi universitari dedicati a tale attività di ricerca. A ciò si aggiungono: Istruzioni persone autorizzate trattamento (con particolare riferimento alla corretta gestione e utilizzo delle credenziali di accesso ai dispositivi e ai file utilizzati nella ricerca); Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); antivirus/firewall; Back – up dei dati

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

La gravità del rischio è **Bassa**. L'impatto sugli interessati potrebbe essere significativo, tuttavia le misure di gestione dell'accesso all'applicativo e le misure adottate a protezione delle postazioni di lavoro riducono notevolmente la probabilità di accadimento. Si consideri che lo studio opera su un data set pseudonimizzato derivante da un'estrazione operata dal Centro Partecipante, presso il quale la fonte originaria dei dati rimane intatta, distinta e non collegata in alcun modo con il data set pseudonimizzato. Pertanto, una modifica indesiderata dei dati nel data set oggetto dello studio non avrebbe impatti sostanziali sui diritti dei pazienti, impatti che, al contrario, sarebbero di non poco conto laddove la modifica indesiderata avesse ad oggetto la fonte originaria. In tal caso, tuttavia, si tratterebbe di un rischio non connesso al trattamento realizzato nello studio.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

La probabilità di concretizzazione del rischio è **Molto bassa**. Con riferimento ad eventuali modifiche indesiderate:
sono adottate misure di sicurezza ICT considerate minime e necessarie dall'AGID, aggiornate periodicamente in linea con il progresso tecnologico, poste a tutela dei sistemi universitari in cui sono conservati i file utilizzati per lo studio.
sono adottate misure di sicurezza degli accessi fisici e degli accessi logici poste a tutela dell'accesso ai dispostivi universitari;
viene effettuato un backup periodico di sistemi e materiale conservato nei server in uso all'Università.
Per evitare, o in ogni caso limitare, possibili modifiche indesiderate ad opera dei membri del gruppo di ricerca o del personale Unimore coinvolto nel Progetto, sono adottate a livello universitario procedure, regolamenti e policy in materia di protezione e corretto trattamento dei dati. Tale materiale è integrato dagli iter e dalle procedure delineate *ad hoc* per la realizzazione del Progetto. Si sottolinea, inoltre, che i sistemi di verifica e controllo sistematico e ripetuto dei dati raccolti, nonché della loro qualità e modalità di elaborazione rendono la probabilità di modifica indesiderata assai remota e mai verificatasi in precedenza nell'attività di ricerca di cui è stato responsabile il PI.

PERDITA DI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Nel caso di specie, una perdita di dati potrebbe riguardare esclusivamente i dati informatici, poiché ogni informazione utilizzata è ricavabile dalle cartelle cliniche cartacee conservate presso il Centro Partecipante, che rimangono intatte e indipendenti dal data set utilizzato ai fini della ricerca.
La perdita del file pseudonimizzato potrebbe eventualmente incidere sull'operatività dello Studio (ad esempio rallentandone lo svolgimento), ma non arrecherebbe alcun danno né allo studio né agli interessati, in quanto le informazioni sono integralmente recuperabili dalla documentazione cartacea originaria e il data set è pseudonimizzato; quindi, la sua perdita non consentirebbe comunque l'identificazione dei soggetti.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Le principali minacce sono di natura informatica: distruzione, cancellazione o corruzione del file (ransomware, blocco temporaneo dei sistemi, guasti hardware al server, malfunzionamenti che compromettono la disponibilità dei dati).

Ulteriori rischi possono derivare da errori umani (uso improprio della posta elettronica che introduce malware, cancellazione accidentale) o da eventi naturali (incendio, allagamento o fulmini che danneggino il datacenter).

Quali sono le fonti di rischio?
Fonti umane interne: operatori che, per errore o inesperienza, cancellano o sovrascrivono dati; postazioni di lavoro lasciate incustodite; errori progettuali che alterano impropriamente i dati.
Fonti umane esterne: attacchi informatici (hacker).
Fonti non umane: virus informatici, calamità naturali, guasti tecnici al datacenter o alla rete elettrica.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Backup periodici; controllo degli accessi (log); antivirus e firewall; misure anti-intrusione; tracciabilità delle operazioni; gestione sicura delle postazioni; formazione e istruzioni alle persone autorizzate; politiche di sicurezza informatica e di tutela della privacy adeguate agli standard richiesti.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

La gravità del rischio è **Bassa**.
Pur potendo la perdita dei dati pseudonimizzati creare discontinuità nello svolgimento dello Studio, non vi sarebbero impatti sui diritti e sulle libertà degli interessati, perché:

- il data set utilizzato è pseudonimizzato e, quindi, non permette in alcun modo l'identificazione dei soggetti;
- la perdita non comporterebbe un danno alla ricerca, poiché tutte le informazioni sono presenti nelle cartelle cliniche cartacee conservate presso il Centro Partecipante, che restano completamente integre e accessibili;
- la fonte originaria dei dati non è mai coinvolta dal trattamento oggetto dello Studio.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

La probabilità è **Molto bassa.**
Le misure tecniche e organizzative adottate (sicurezza ICT AGID, sistemi aggiornati, backup periodici, misure fisiche e logiche di controllo degli accessi) rendono altamente improbabile la perdita.
In ogni caso, anche qualora si verificasse un evento di questo tipo, la perdita non sarebbe mai definitiva, potendo il file pseudonimizzato essere ricostruito sulla base delle cartelle cliniche cartacee e delle copie di backup.

PROBABILITA' (P)	***IMPATTO (I)***	***RISCHIO (R=P*I)***
Probabilità molto bassa: 1	Impatto molto basso: 1	
Probabilità bassa: 2	Impatto basso: 2	Rischio basso: R< 7
Probabilità media: 3	Impatto medio: 3	Rischio medio: 7<R<11
Probabilità alta: 4	Impatto alto: 4	Rischio alto: R>11
Probabilità molto alta: 5	Impatto molto alto: 5	

A CURA DEL DPO

MATRICE DI VALUTAZIONE DEL RISCHIO

		IMPATTO§§				
PROBABILITA'	**MOLTO ALTO§**	5	10	15	20	25
	ALTO	4	8	12	16	20
	MEDIO	3	6	9	12	15
	BASSO	2	4	6	8	10
	MOLTO BASSO	1	2	3	4	5
		MOLTO BASSO	**BASSO**	**MEDIO**	**ALTO**	**MOLTO ALTO**

§ Frequenza con la quale si possono verificare criticità nel trattamento dei dati: **Rischio molto basso**: è probabile che non si verifichi mai; **Basso**: non è probabile che si verifichi, ma può accadere; **Medio**: si può verificare occasionalmente; **Alto**: è probabile che si verifichi, ma non in modo persistente/stabile; **Molto alto**: è quasi certo che si verifichi, possibilmente in modo frequente
§§ Impatto atteso: **Molto basso**: è improbabile che possa avere un qualsiasi impatto; **Basso**: può avere un impatto; **Medio**: è probabile che abbia un impatto; **Alto**: molto probabile che abbia un impatto significativo; **Molto alto**: correlato ad un impatto maggiore

MINACCIA	VALORE DEL RISCHIO (P*I)	LIVELLO DI RISCHIO	VALUTAZIONE COMPLESSIVA
ACCESSO ILLEGITTIMO	1*2	2	6
MODIFICHE INDESIDERATE DEI DATI	1*2	2	
PERDITA DI DATI	1*2	2	

Classificazione	Intervallo del rischio
Assenza di Rischio	Valore finale tra 0 e 1 compresi
Rischio Basso	Valore finale tra 2 e 6 compresi
Rischio Medio	Valore finale tra 7 e 11 compresi
Rischio Elevato	Valore finale tra 12 e 16 compresi