VALUTAZIONE D'IMPATTO PER PROGETTI DI RICERCA IN AMBITO SANITARIO

PER STUDI INTERVENTISTICI

(ART. 35 Regolamento UE 2016/679)

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, ai sensi dell'art.35 Regolamento UE 2016/679 (GDPR), deve sempre essere effettuata quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, 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.

Una valutazione d'impatto negli studi interventistici andrà dunque sempre condotta quando, ricorrono almeno 2 dei seguenti elementi:

- trattamenti di dati sanitari,
- trattamenti di dati relativi a soggetti vulnerabili (esempio: minori; soggetti con malattie psichiatriche; anziani),
- trattamenti su larga scala,
- utilizzo di nuove tecnologie (esempio: utilizzo di AI)

A CURA DEL RICERCATORE

Titolo dello studio: Scomporre la complessità delle malattie infiammatorie intestinali (IBD) – Studio prospettico con focus sul rischio cardiovascolare

Codice di Protocollo: DICOM-IBD_RF-2024-12377843

Titolare del trattamento: Policlinico San Donato S.p.A.

Principal Investigator: Prof. Vito Annese

Co-Principal Investigator: Dott.ssa Serenella Castelvecchio

Unità: Gastroenterologia ed Endoscopia Digestiva / Cardiologia Preventiva e Medicina di Genere

Data compilazione: 05/05/2026

TRATTAMENTO DEI DATI		
Descrizione del trattamento		
Sinossi dello Studio		
	Obiettivi e Finalità	Studiare pazienti con IBD afferenti agli ambulatori della Gastroenterologia e valutare durante il follow-up l'incidenza di eventi cardiovascolari maggiori (es. infarto, ictus, ischemia miocardica) rispetto ad una popolazione comparabile per sesso ed età senza IBD già in follow-up (studio CV-PREVITAL) con il Co-PI. Saranno valutati con appositi questionari i classici fattori di rischio (personali e familiari), stile di vita (dieta, fumo, attività fisica, ecc.), caratteristiche delle IBD (attività, terapia), parametri biochimici/metabolici (colesterolo, HBA1c, ecc.) ed inoltre una valutazione multi-omica (genomica, metabolomica del microbiota, trascrittomica sulle biopsie endoscopiche e proteomica) con particolare attenzione ai soggetti che hanno sviluppato gli eventi cardiovascolari. Qualora alla valutazione basale o durante il follow-up si documenti comunque un elevato rischio cardiovascolare, i pazienti saranno valutati dal cardiologo per ulteriori indagini. L'obiettivo finale sarà consentire per la prima volta una stima prospettica in Italia di questo rischio nelle IBD, ma soprattutto di cercare di correlare il rischio a specifici bio-marcatori, ed in definitiva potenzialmente di migliorare la valutazione del rischio prognostico rispetto al classico SCORE 2.
	Popolazione	<u>Criteri di inclusione</u> - Pazienti che hanno firmato il consenso informato - Età compresa tra 18 e 80 anni - Diagnosi confermata di Colite Ulcerosa o malattia di Crohn Popolazione di controllo (studio CV-PREVITAL) - Età ≥ 18 anni <u>Criteri di esclusione</u> - Diagnosi incerta di IBD - Impossibilità di firmare il consenso informato - Non disponibilità a fornire campioni di sangue e feci o a sottoporsi a valutazioni endoscopiche periodiche Popolazione di controllo (studio CV-PREVITAL) - Malattia cardiovascolare in atto o pregressa (storia personale di infarto del miocardio, angina pectoris, interventi di rivascolarizzazione arteriosa, ictus, TIA, arteriopatia obliterante arti inferiori) - Patologie psichiatriche - Patologie neoplastiche e/o degenerative in fase evolutiva
	Disegno dello Studio	Studio di intervento con raccolta di materiale biologico, monocentrico.
	Numero di Soggetti	±300 vs altrettanti controlli senza IBD

	Follow-up | 2 anni **Durata dello Studio** | 3 anni
Tipologia di dati raccolti	
Modalità di raccolta *(fonte dei dati) (barrare anche più caselle)*	☒ direttamente dall'interessato ☐ ricevute da terze parti Specificare: _____
Trattamento dei dati *(indicare il supporto utilizzato per la rilevazione e conservazione dei dati)*	☒ In formato cartaceo ☒ In formato digitale ☐ In formato cartaceo / digitale ☐ altro (specificare) _____
Categorie di persone interessate	☒ pazienti ☐ *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/o le condizioni socioeconomiche ☐ informazioni su istruzione e formazione professionale ☐ anamnesi lavorativa ☐ informazioni su religione o altre credenze ☐ *altro (specificare)* _____
I dati personali (anche pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati/condivisi con altri?	☒ No ☐ Sì In caso positivo, selezionare uno o più ambiti di comunicazione: ☐ Promotore ☐ Altri centri partecipanti ☐ CRO
I dati personali (anche pseudonimizzati e che non siano	☒ No ☐ Sì

pertanto anonimi o aggregati) vengono trasferiti all'estero?	Se sì ☐ Paesi area UE ☐ Paesi extra UE In quale/i Paese/i all'interno dell'area o extra UE _____
Vengono impiegate particolari tecnologie nel trattamento dei dati personali (es: AI) ?	☐ No ☒ Sì Descrivere: implementazione di un modello di Intelligenza artificiale _____

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 o altri soggetti autorizzati, possono (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 ☐ Sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati

	☐ Altro (specificare) _____
Descrivere, se del caso, le specifiche misure di sicurezza adottate e relative alla particolare tecnologia utilizzata	

PRINCIPI, FINALITA' E BASI GIURIDICHE	
Necessità e proporzionalità	
Gli scopi del trattamento sono specifici, espliciti e legittimi?	X Sì ☐ No Motivare la risposta: 1. Specificità degli scopi: Gli scopi del trattamento sono chiaramente e analiticamente definiti all'interno del protocollo. In relazione agli obiettivi dello studio il trattamento è legato esclusivamente alla ricerca così come dettagliatamente descritta e non a ulteriori scopi; pertanto, le finalità risultano circoscritte al contesto descritto. L'uso dei dati è confinato a uno scopo ben definito e non a fini generici o non correlati. 2. Esplicitazione degli scopi: Gli scopi del trattamento sono comunicati chiaramente negli endpoints del protocollo. Gli stessi sono funzionali a raccogliere evidenze scientifiche, migliorare la comprensione delle patologie/trattamenti descritti, e i relativi dati saranno trattati in modo proporzionale all'obiettivo. 3. Legittimità degli scopi: Per quanto riguarda la legittimità, lo studio deve rispettare i requisiti legali per la ricerca scientifica previsti dal GDPR e dalle normative nazionali applicabili. Poiché il trattamento è finalizzato alla ricerca, e non a scopi commerciali, rientra nelle finalità legittime ai sensi dell'art. 9 del GDPR, che consente il trattamento di dati sanitari per motivi di ricerca scientifica, soggetto all'adozione di adeguate misure di sicurezza e minimizzazione dei dati. 4. Proporzionalità e necessità: Riguardo a proporzionalità e necessità, i dati trattati sono strettamente necessari a raggiungere gli obiettivi dello studio. L'utilizzo di dati anonimi o pseudonimizzati, ove applicabile, sarà sempre impiegato quale misura di mitigazione per limitare il rischio.
I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	X Sì ☐ No Motivare la risposta: La valutazione circa la pertinenza, limitazione e necessità in relazione alle finalità dello studio in oggetto è basata sul principio di minimizzazione dei dati (art. 5(1)(c) del GDPR): 1. Adeguatezza dei dati: I dati raccolti sono appropriati per raggiungere le finalità dello studio. Nello studio descritto, significa che i dati selezionati oggetto di trattamento sono strettamente necessari per rispondere ai quesiti oggetto della ricerca e alle ipotesi formulate nel protocollo. I dati trattati per finalità di ricerca sono scelti in base alla loro rilevanza scientifica e clinica rispetto agli obiettivi dello studio. 2. Pertinenza dei dati:

	I dati sono pertinenti ovvero hanno un legame diretto con gli scopi dello studio. Gli stessi sono rilevanti per rispondere agli specifici quesiti scientifici che lo studio intende esplorare. Non vengono trattati dati che non hanno una connessione chiara con le finalità dichiarate, riducendo il trattamento a informazioni essenziali per la validità scientifica dello studio. 3. Limitazione dei dati (minimizzazione): Il protocollo prevede la raccolta dei soli dati strettamente necessari per conseguire le finalità dello studio. I dati sono limitati per ridurre l'impatto sulla privacy degli interessati, evitando la raccolta di informazioni sovrabbondanti o ridondanti. Si farà ricorso a tecniche di anonimizzazione o pseudonimizzazione, ove applicabile, per limitare l'identificabilità degli individui. 4. Necessità dei dati: Relativamente al principio di necessità lo studio non potrebbe essere condotto correttamente senza il trattamento dei dati previsti dal protocollo. Ogni categoria di dato trattato è necessaria per fornire risultati significativi e validi scientificamente. La raccolta di ulteriori dati fuori protocollo non essenziali non sarebbe in alcun modo giustificata. Pertanto, è possibile considerare i dati adeguati perché appropriati allo scopo dello studio, pertinenti perché direttamente legati alle finalità dichiarate e limitati in quanto raccolti solo nella misura strettamente necessaria per la ricerca, nel rispetto del principio di minimizzazione dei dati previsto dal GDPR.
Integrità ed esattezza	
I dati sono esatti e aggiornati?	X Sì ☐ No Motivare la risposta: La valutazione rispetto alla correttezza dei dati e all'aggiornamento è stata fatta in linea con il principio di esattezza previsto dall'art. 5(1)(d) del GDPR: 1. Esattezza dei dati: Lo studio si basa su dati clinici, in un contesto finalizzato alla diagnosi e cura del paziente. Il Codice di Deontologia Medica, nonché le responsabilità civili e penali che potrebbero derivare dal trattamento di dati inesatti, sono presidi che assicurano massima cura nella verifica dell'esattezza e accuratezza dei dati. Vengono applicate procedure per la revisione e la verifica dei dati clinici, riducendo così il rischio di errori. 2. Controlli e verifiche incrociate: All'interno dello studio, sono attuati meccanismi di controllo per garantire l'esattezza dei dati utilizzati. Processi di revisione e pulizia dei dati sono posti in essere per assicurare che non vi siano errori evidenti o duplicazioni [selezionare se del caso tra 4-Eyes Check, Double Data Entry, Source Data Verification (SDV), Query Management, Edit Checks, Audit Trail, Risk-Based Monitoring, Statistical Data Cleaning, Validation and Cross-Validation] 4. Aggiornamento dei dati:

	I dati sono raccolti e periodicamente controllati e aggiornati per assicurare la conformità del risultato. Operando in un contesto finalizzato alla diagnosi e cura del paziente tale operazione è rigorosa e metodica. 5. Misure di mitigazione del rischio: Esclusivamente i dati accurati e affidabili vengano inclusi nelle analisi finali: lo studio adotta misure di mitigazione come l'esclusione di record non completi o poco chiari. Pertanto i dati trattati nello studio sono esatti perché raccolti in un contesto affidabile e rigoroso, con obblighi precisi derivanti dalla legge e dalla deontologia. Inoltre, lo studio prevede misure per verificare la correttezza dei dati e garantire che qualsiasi eventuale errore venga identificato e corretto.
Limitazione della conservazione	
Per quanto tempo verranno conservati i dati raccolti?	5 anni Decorso tale termine i dati verranno: ☒ Anonimizzati completamente ☐ Distrutti ☐ altro (*specificare*) _____

Basi giuridiche	
Quali sono le basi giuridiche del trattamento?	☒ art. 9, par. 2, lett. a) GDPR[1]
MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO	
Informativa e consenso	
Come sono informati del trattamento gli interessati?	☐ Informativa consegnata direttamente all'interessato
E' stata predisposta una valutazione di impatto ai sensi dell'art. 35 del GDPR?	☒ si ☐ no
Esercizio da parte dell'interessato dei diritti ex artt.15-22 DPR	
E' stata predisposta una procedura ad hoc da parte del Titolare?	☒ Sì ☐ No
Come fanno gli interessati a esercitare i loro diritti	Rivolgendosi direttamente ai titolari del trattamento o ai rispettivi dpo così come indicato nell'informativa

[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.

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO		
MISURA	Esistenti	Note
Organigramma interno	X	○ Ruoli e Responsabilità
Controllo accessi	X	○ L'accesso avviene tramite account personali. ○ Sono applicate politiche di minimizzazione e restrizione dell'accesso ai dati personali. ○ L'autenticazione è effettuata tramite password e, in alcuni casi, tramite autenticazione a due fattori. ○ Sono adottate delle politiche di complessità delle password in coerenza con le buone pratiche di settore
Gestione dei cambiamenti	X	○ Ogni modifica ai sistemi IT è valutata, registrata e monitorata. ○ E' stata definita una procedura generale per la protezione dei dati personali, comprensiva di valutazioni in ottica by design e by default, volta a individuare i requisiti di protezione dei trattamenti e a implementare e mantenere i sistemi e le applicazioni garantendo livelli di sicurezza adeguati. ○ L'acquisizione di componenti del sistema informativo tiene conto dei requisiti di sicurezza dei trattamenti che dovranno essere supportati e delle garanzie offerte dal fornitore.
Strumenti di sicurezza e protezione	X	○ Firewall, anti-malware centralizzati e strumenti di protezione per le postazioni di lavoro. ○ Monitoraggio continuo del sistema IT per rilevare incidenti di sicurezza.
Gestione degli incidenti	X	○ Le violazioni dei dati personali vengono gestite tramite procedure di escalation, coinvolgendo il DPO. ○ È attivo un sistema di monitoraggio continuo (SIEM e SOC) per raccogliere e analizzare i log. ○ Il titolare mantiene un registro delle violazioni dei dati personali.
Rapporti con i Responsabili	X	○ Il titolare gestisce i rapporti con i propri Responsabili del trattamento attraverso accordi formalizzati che comprendono specifiche clausole per assicurare la riservatezza dei dati trattati e l'obbligo per i Responsabili di operare in conformità alla normativa sul trattamento dei dati personali, in particolare, per quanto riguarda le misure di sicurezza, in riferimento agli art. 28 e 32.

Pseudonimizzazione e cifratura	X	○ Pseudonimizzazione e cifratura sono utilizzate per limitare l'identificabilità dei dati. ○ Viene applicata la cifratura nelle connessioni VPN, nei servizi HTTPS e nelle comunicazioni machine-to-machine.
Continuità operativa	X	○ L'infrastruttura IT è progettata per garantire la continuità operativa tramite due datacenter distanti almeno 20 km. ○ I dati di backup sono conservati in un sito di recupero dati a oltre 100 km.
Formazione e gestione del personale	X	○ Il personale riceve formazione istituzionale con corsi FAD sulla protezione dei dati e sicurezza informatica, con incontri di aggiornamento periodici awareness e sensibilizzazione. ○ Il personale con ruoli specifici nell'ambito della data protection (Local Privacy Executive e Local Privacy Contact) riceve una formazione specifica ulteriore.
Sicurezza delle postazioni di lavoro e delle reti	X	○ Le postazioni di lavoro sono aggiornate regolarmente e protette da sistemi anti-malware. ○ Le reti sono protette da firewall e strumenti di monitoraggio delle intrusioni.
Backup e Vulnerability Assessment	X	○ Backup giornalieri dei dati e test periodici del sistema di ripristino. ○ Valutazioni periodiche della vulnerabilità per identificare possibili rischi di sicurezza.
Sicurezza fisica	X	○ I datacenter sono protetti da misure fisiche e ambientali (protezione da incendi, allagamenti, controllo accessi fisici). ○ I datacenter sono certificati TIER3 e TIER4.

APPENDICE

MINACCE

ACCESSO ILLEGITTIMO AI DATI

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

Impatti Potenziali
Perdita di controllo dei propri dati
Utilizzo da parte di terzi di dati dell'interessato

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minaccia
Comportamenti sleali/fraudolenti
Attacco informatico (es. social engineering, man in the middel, denial of ervice, brute force, etc.)
Furto e/o perdita di dispositivi, supporti di memorizzazione, documenti

Quali sono le fonti di rischio?

Fonte
Fonti umane esterne (es. criminali informatici, fornitori, utenti)
Fonti umane interne accidentali (es. collaboratori negligenti)

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; Crittografia; Pseudonimizzazione

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	Importante
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	Limitato

MODIFICHE INDESIDERATE DEI DATI

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

Impatti Potenziali
Dati non esatti e/o non aggiornati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minaccia
Errore operativo

Fonte
Fonti umane interne accidentali (es. collaboratori negligenti)

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; Back – up dei dati

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?	Limitato
Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?	Trascurabile

PERDITA DI DATI

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Una perdita dei dati potrebbe causare l'alterazione dei risultati dello Studio o la impossibilità di proseguire lo Studio

Impatti Potenziali
Costi aggiuntivi

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

Minaccia
Errore operativo

Quali sono le fonti di rischio?

Fonte
Eventi tecnologici (es. guasti, malfunzionamenti, etc.)
Fonti umane interne accidentali (es. collaboratori negligenti)

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

Back – up dei dati; Controllo accessi (log); Misure anti – intrusive; antivirus/firewall; Tracciabilità, Gestione postazioni; Politiche di tutela della privacy¸ Politiche di sicurezza informatica

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	Trascurabile
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	Trascurabile

VALUTAZIONE DEL RISCHIO

PROBABILITA' (P)	*IMPATTO (I)*	*RISCHIO (R=P*I)*
Probabilità trascurabile: 1 Probabilità limitato: 2 Probabilità importane: 3 Probabilità massima: 4	Impatto trascurabile: 1 Impatto limitato: 2 Impatto importante: 3 Impatto massimo: 4	Rischio basso: R< 6 Rischio medio: 7<R<11 Rischio alto: R>11

MATRICE DI VALUTAZIONE DEL RISCHIO

		IMPATTO§§			
PROBABILITA' §	**MASSIMO**	4	8	12	16
	IMPORTANTE	3	6	9	12
	LIMITATO	2	4	6	8
	TRASCURABILE	1	2	3	4
		TRASCURABILE	**LIMITATO**	**IMPORTANTE**	**MASSIMO**

§ 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;

§§ 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;

MINACCIA	**VALORE DEL RISCHIO (P*I)**	**LIVELLO DI RISCHIO**	**VALUTAZIONE COMPLESSIVA** (SOMMA COLONNA LIVELLO RISCHIO)
ACCESSO ILLEGITTIMO	3*2	6	**6**
MODIFICHE INDESIDERATE DEI DATI	1*2	2	
PERDITA DI DATI	1*1	1	

Classificazione	**Intervallo del rischio**
Assenza di Rischio	Valore finale tra 0 e 2 compresi
Rischio Limitato	Valore finale tra 3 e 6 compresi
Rischio Importanto	Valore finale tra 7 e 11 compresi
Rischio Massimo	Valore finale tra 12 e 16 compresi