VALUTAZIONE D'IMPATTO PER PROGETTI DI RICERCA IN AMBITO SANITARIO SU DATI RETROSPETTIVI

(ART. 110 D. LGS. 196/2003 s.m.i., Provvedimento Garante n. 146/2019)

La valutazione di impatto (DPIA- data protection impact assestment) 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 Trial di Emulazione sulla Terapia della Meningite Batterica

Codice di Protocollo NO CODICE

Titolare del trattamento: AZIENDA OSPEDALIERO-UNIVERSITARIA DI MODENA

Struttura/Dipartimento/U.O./Servizio S.C. di Malattie Infettive

Soggetto delegato: Dott.ssa Marianna Meschiari

Promotore: AOU di Modena

Data compilazione 16/09/2024

TRATTAMENTO DEI DATI	
Descrizione del trattamento *(compilare i campi successivi)*	
Obiettivi dello studio	Questo studio mira ad affrontare in modo esaustivo la meningite batterica nella popolazione adulta italiana, concentrandosi sulla sua epidemiologia, caratteristiche cliniche, fattori predisponenti, agenti eziologici e outcomes.
Breve sintesi del progetto	Studio di coorte storica retrospettiva; per il centro di Modena, il numero stimato dei pazienti potenzialmente arruolabili è di circa 200.
Promotore	AOU di Modena
Tipologia di dati raccolti	

Modalità di raccolta *(barrare anche più caselle)*	**X** consultazione cartelle cliniche/documentazione sanitaria **X** archivi di dati clinici **X** archivi di test diagnostici **X** dati di laboratorio ☐ altro (specificare)_____
Trattamento dei dati *(indicare il supporto utilizzato per la rilevazione e conservazione dei dati*	☐ In formato cartaceo X In formato digitale ☐ altro (specificare) _____
Categorie di persone interessate	X Pazienti maggiorenni con meningite batterica accertata afferenti agli ospedali dei centri partecipanti negli ultimi 10 anni. ☐ persone sane ☐ operatori sanitari ☐ soggetti vulnerabili ☐ altro (specificare) _____
Categorie di dati trattati	X 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 (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati/condivisi con altri?	X No ☐ Sì Se sì, selezionare uno o più ambiti di comunicazione: ☐ Promotori ☐ CRO ☐ altro (specificare) _____
I dati personali (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono trasferiti all'estero?	X No ☐ Sì 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 soggetti dello studio?	☐ No **X** Sì Se sì, specificare le ragioni sottese a tale esigenza: I dati identificativi dei pazienti arruolati vengono conservati a cura del PI nella patient identification list e distrutti al termine dello Studio

Descrivere le procedure utilizzate per ***a) non identificare direttamente o pseudonimizzare*** ***b) rendere anonimi i dati dei partecipanti nelle diverse fasi della ricerca***	a) Per non identificare direttamente l'interessato o pseudonimizzare sono adottate le seguenti misure: ☐ Adozione di tecniche crittografiche (dei dati identificativi del soggetto) X 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_____ b) Per rendere anonimi 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)_____

PRINCIPI, FINALITA' E BASI GIURIDICHE	
Necessità e proporzionalità	
Sono trattati solo i dati necessari e pertinenti al perseguimento delle finalità della ricerca (Minimizzazione)?	X 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?	X 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 _____ 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. j) GDPR[1] ☐ art. 110, co. 1 primo periodo Codice Privacy[2]

[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

	X art. 110, co. 1, secondo periodo Codice Privacy[3]

MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO	
Informativa e consenso	
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 **(barrare una o entrambe le motivazioni qua sotto)**: X del numero molto alto di interessati che è stato stimato X deceduti o non contattabili
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 GDPR	
E' stata predisposta una procedura ad hoc da parte dell'Ente?	X Sì ☐ No

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO (standardizzare per singola Azienda)		
MISURA	Esistenti	Note
Organigramma interno	X	Delibera 150 del 06.09.2018
Nomine responsabili esterni	Non sono presenti	
Nomina DPO	X	Delibera 90 del 16.05.2018
Informativa	X	Sempre
Istruzioni persone autorizzate trattamento	X	Le persone autorizzate al trattamento saranno formate dal PI
Formazione	X	Sarà effettuato un self-training
Registri	X	Non sono presenti dei registri specifici
Procedure	X	Non sono presenti delle procedure specifiche
Politiche di tutela della privacy	X	AOUMO ha nominato un DPO e all'interno dell'Azienda esiste un Gruppo aziendale Privacy - al quale afferiscono, tra gli altri membri, il Direttore del Servizio Tecnologie dell'Informazione e il Referente aziendale Data Breach - che ha il compito di garantire e coordinare le attività aziendali correlate alla normativa in materia di protezione dei dati personali, supportando il Titolare del

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.

		trattamento negli adempimenti previsti dalla normativa (Regolamento EU 2016/679, Decreto Legislativo 196/2003 e s.m.i.). Il Responsabile del Settore legale, assicurazioni e privacy si interfaccia con il Data Protection Officer e coordina il Gruppo aziendale Privacy. L'Azienda ha dottato un Regolamento in materia di Protezione Dati (Delibera 216 del 20/12/2019)
Distruzione/smaltimento sicuro cartaceo	X	Non pertinente
Inventario degli asset	X	Le postazioni di lavoro aziendali sono censite nel programma di gestione aziendale. Non è prevista una abilitazione specifica per le postazioni utilizzate per l'accesso alla cartella condivisa
Misure anti – intrusive (cartelli di divieto di accesso ai locali, strumenti per la rilevazione degli accessi, guardiania, portineria, serrature armadi, schedari, ecc.)	X	I sistemi server sono ospitati presso il Data Center aziendale che risponde ai requisiti tier 3 ed anche i Datacenter regionali gestiti da Lepida S.c.p.A rispondono ai requisiti tier 3.
Politiche di sicurezza informatica	X	Sulle postazioni aziendali e sul file server viene garantito l'aggiornamento dei Sistemi Operativi e di un programma di antivirus e di anti-malware completo. Sul file server è anche attivo il firewall locale
Controllo accessi (log)	X	Essendo una cartella condivisa non sono presenti politiche di audit all'accesso
Antivirus / firewall	X	Presente sul firewall del file server
Politiche di clear screen	X	Non pertinente
Back – up dei dati	X	La cartella condivisa utilizzata come unità di memorizzazione dello studio è situata nei file server aziendali e viene quotidianamente salvata attraverso le normali procedure di Backup aziendali su due copie, una locale e una remota presso il datacenter di Lepida di Ferrara
Politiche di trasmissione dei dati	x	Per questo studio non vengono trasmessi i dati all'esterno dell'Azienda Ospedaliero Universitaria di Modena
nel caso si utilizzi un sito web esterno:	x	Per questo studio non si usa un sito web esterno
Connessione sicura	x	La cartella condivisa è accessibile solo dall'interno dell'Azienda AOUMO
Accesso protetto da utenza personale		La cartella condivisa è accessibile ai soli utenti autorizzati e identificati con credenziali di Active Directory
Crittografia	x	Lo strumento utilizzato per la raccolta dati (Excel) non prevede la crittografazione
Pseudonimizzazione		I dati dei pazienti saranno pseudonimizzati e il soggetto verrà identificato con un codice identificativo composto da due lettere (sigla della città del centro) e da un numero progressivo.
Sicurezza dei documenti cartacei	X	I dati non vengono raccolti in formato cartaceo
Gestione postazioni	X	Le postazioni sono accessibili dai soli utenti aziendali. è presente un disciplinare aziendale sull'utilizzo delle postazioni informatiche

Autenticazione	X	L'autenticazione avviene tramite username/password. La password è cambiata ogni 90 giorni secondo le normative vigenti
Policy di gestione data breach	X	L'Azienda ha adottato una procedura di gestione delle violazioni dei dati personali in cui sono definite le modalità operative da seguire in caso di incidente. La medesima procedura viene fornita ai Responsabili del trattamento in quanto disciplina anche le violazioni esterne all'Azienda. È previsto un registro aziendale delle violazioni
Altro:		

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 aziendali 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; virus

Quali sono le fonti di rischio?

Fonti umane interne (lasciare incustodita la postazione di lavoro, 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; Crittografia; Pseudonimizzazione

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

Bassa: l'impatto sugli interessati potrebbe essere elevato, tuttavia le misure previste per evitare gli accessi non autorizzati rendono limitata la probabilità di accadimento

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

Molto bassa: le politiche di sicurezza informatica e le misure adottate a protezione delle postazioni di lavoro e degli archivi cartacei rendono quasi nulla la probabilità di accadimento

MODIFICHE INDESIDERATE DEI DATI

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

Perdita di integrità del dato; la modifica potrebbe essere definitiva e avere conseguenze sulla attendibilità dei risultati dello studio fino a conseguenze sulla cura dei pazienti

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Utilizzo inappropriato delle password di accesso ai pc aziendali 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; virus

Quali sono le fonti di rischio?

Fonti umane interne (lasciare incustodita la postazione di lavoro, 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?

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, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Bassa: l'impatto sugli interessati potrebbe essere elevato, 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.

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

Molto bassa: le misure adottate a protezione delle postazioni di lavoro rendono quasi nulla la probabilità di accadimento,

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; tuttavia non si tratta di dati originali

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

La minaccia principale è quella di una distruzione o cancellazione erronea o volontaria dei dati
Le principali minacce possono essere di natura informatica (infezione da ransomware che blocca il sistema di accesso ai propri data base, provocando anche solo in modo temporaneo una impossibilità ad accedere al server, guasto che determina il danneggiamento, l'interruzione o la non disponibilità del sistema, che andando a colpirne elementi chiave possa mettere a rischio la disponibilità dei dati) o derivare da una azione umana (utilizzo improprio della posta elettronica da parte di un operatore attraverso cui un virus potrebbe bloccare il sistema aziendale; Incidente tecnico al datacenter (incendio, inondazione, fulmini…)

Quali sono le fonti di rischio?

Fonti umane interne (operatori autorizzati che abusino del proprio ruolo o colposamente operino cancellazioni sui dati per inesperienza o imperizia; lasciare incustodita la postazione di lavoro; errore progettuale/realizzativo che opera una modifica impropria ai dati gestiti); Fonti umane esterne (hacker); Fonti di rischio non umane (virus informatico; calamità naturali; guasto all'impianto elettro-idraulico del datacenter)

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?

Molto bassa: i dati non sono originali, quindi l'impatto sugli interessati non è elevato, inoltre le misure previste per evitare la perdita dei dati rendono limitata la probabilità che essa si verifichi

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

Molto bassa: le misure adottate a protezione delle postazioni di lavoro rendono quasi nulla la probabilità di accadimento

VALUTAZIONE DEL RISCHIO

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

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** (SOMMA COLONNA LIVELLO RISCHIO)
ACCESSO ILLEGITTIMO	2*1	2	**5**
MODIFICHE INDESIDERATE DEI DATI	2*1	2	
PERDITA DI DATI	1*1	1	

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