ESTRATTO DELLA VALUTAZIONE DI IMPATTO

1. Informazioni generali

1.1 Titolare del trattamento

La presente DPIA è stata redatta dalla Fondazione S. Matteo, in qualità di Titolare del trattamento ("Titolare del trattamento" o "Fondazione").
Tale ruolo è assunto in quanto la Fondazione è il promotore dello studio, avendone determinato finalità e mezzi di trattamento.
Il Principal Investigator (Responsabile dello studio) è la dott.ssa *Catherine Klersy.*

1.2 Contesto di riferimento

Oggetto della presente valutazione d'impatto (Data Protection Impact Assessment – DPIA) è il trattamento dei dati personali dei pazienti ricoverati presso il Policlinico San Matteo della Fondazione nel periodo compreso tra il 01-01-2020 e il 31-12-2022, al fine di condurre uno studio clinico osservazionale retrospettivo per derivare e convalidare un modello di predizione clinica per la sepsi intraospedaliera

Tale studio sarà multicentrico coordinato dalla Fondazione.

1.3 Standard di riferimento per la predisposizione della DPIA

Si rimanda alla procedura aziendale.

1.4 Descrizione del quadro normativo e regolatorio, standard e buone prassi

Si rimanda alla procedura aziendale.

1.5 Team di lavoro

Il presente documento è stato redatto da un team della Sperimentazione e sottoscritto dal Direttore Generale e Direttore Scientifico della Fondazione IRCCS Policlinico San Matteo.

2. Fase 1: Descrizione del trattamento

2.1.1 Il trattamento oggetto della Valutazione di Impatto

Si fa riferimento al protocollo di studio dal titolo *"Predittori per la sepsi ospedaliera. Uno studio di coorte longitudinale del nodo OHDSI italiano" - OMOP_SEPSIS" [OMOP_SEPSIS*, Version *1.0 of date (24/10/2023)]* e documentazione studio specifica.

2.1.2 Ruoli e responsabilità collegate al trattamento.

Università degli studi di pavia: responsabile del trattamento per conto della Fondazione IRCCS;
Biomeris srl: responsabile del trattamento per conto della Fondazione IRCCS;
Ognuno dei due responsabili tratta stime statistiche aggregate dai Centri partecipanti e si occupa tramite un'analisi "federata" di combinare queste stime
Vi sono altri soggetti (Comitato Etico, AIFA) che possono intervenire nel processo per le verifiche di competenza.

In ogni caso il personale che accede ad archivi contenenti dati personali anche solo indirettamente identificativi è stato autorizzato se subordinato/parasubordinato oppure nominato Responsabile ex art. 28 GDPR negli altri casi.

2.2 Dati, processi e beni di supporto

Si fa riferimento al protocollo di studio e documentazione studio specifica; in particolare le informazioni sono riportate nel protocollo [paragrafo *3.3 Study procedures* a pagina 14] e documentazione studio specifica.

2.2.1 **Beni di supporto** (completare solo in caso in cui non sia contenuto in protocollo e documentazione di studio)

- Si fa riferimento al protocollo di studio [paragrafo *7.2 Data recording and source data* pagina 21] e documento n°prot 0067395/24 [Valutazione d'impatto ai sensi dell'art. 35 del GDPR

  relativa alla realizzazione di una piattaforma secondo lo standard OMOP/OHDSI]

3. Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento

3.1 Proporzionalità e necessità

Lo scopo di miglioramento del processo di cura/prevenzione e più in generale della salute della collettività si viene a contrappore al diritto alla riservatezza dei singoli. Il miglioramento è tanto più urgente quanto le patologie hanno effetti socioeconomici importanti. D'altra parte, gli impatti sui pazienti sono tanto maggiori quanto le patologie destano allarme sociale e potenziale discriminazione.

I dati personali sono indispensabili per la qualità della ricerca. Le fasi di verifica dei risultati sono un requisito fondamentale di un processo di qualità. Queste, quindi, richiedono una collegabilità del dato alle informazioni cliniche primarie e di conseguenza all'identità del paziente. La strategia principale per rendere il trattamento il meno impattante possibile sulla riservatezza è la minimizzazione della collegabilità tramite tecniche di minimizzazione e pseudonimizzazione dei dati.

3.1.1 Finalità esplicite e legittime

Le finalità del trattamento sono di ricerca scientifica.

3.1.2 Fondamenti legali del trattamento

Art. 110 bis c. 4 d.lgs. 196/2003

3.1.3 I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario al conseguimento delle finalità del trattamento ("Minimizzazione dei dati")

Si rimanda alla procedura aziendale.

3.1.4 Accuratezza ed aggiornamento dei dati

I dati sono raccolti e trattati da un numero ristretto di persone: Principal Investigator e personale del gruppo di ricerca autorizzato.
Si assume che la documentazione clinica di origine (data warehouse ospedaliero) sia accurata (documento di fede privilegiata).
Le procedure di data quality previste sono tese a verificare queste proprietà del dato.

I dati verranno trattati mediante processo di pseudonimizzazione, ovvero ad ogni soggetto partecipante allo studio verrà assegnato un codice che verrà utilizzato nello studio, come descritto nel documento n°prot 0067395/24. La chiave per risalire ai soggetti sarà conosciuta solo dal Principal Investigator e dai ricercatori del gruppo di ricerca autorizzati dal PI.
I dati raccolti saranno aggregati e verranno considerati solamente i conteggi superiori a 30 pazienti per la pubblicazione e alla fine dello studio.

3.1.5 Durata della conservazione dei dati

Si rimanda alla procedura aziendale.

3.2 Controlli per proteggere i diritti degli interessati

3.2.1 Come sono informati gli interessati circa il trattamento

Si rimanda all'informativa disponibile sul sito internet.

3.2.2 Esercizio dei diritti da parte degli interessati

Si rimanda all'informativa disponibile sul sito internet.

3.2.3 Obbligazioni dei responsabili del trattamento

I responsabili al trattamento dei dati personali sono stati opportunamente nominati.

3.3 Trasferimenti al di fuori dello SEE

Non vi sono trasferimenti extra SEE.

4. Fase 3: Calcolo del livello del rischio

Il livello del rischio e le relative misure di mitigazione viene calcolato utilizzando il tool ENISA disponibile al link: https://redcap.link/calcololivellodelrischiosmatteo
Il documento risultante si allega alla presente quale parte formale e sostanziale della presente DPIA.

5. Fase 4: Calcolo del rischio residuo, piano di remediation e parere del DPO

5.1 Rischio residuo

Si ritiene che il rischio residuo collegato al trattamento di dati personali per le finalità dello studio in oggetto sia accettabile in quanto sono state adottate misure di sicurezza tecniche e organizzative idonee a contenere il rischio per i diritti e le libertà degli interessati.

5.2 Piano di remediation

Per la minimizzazione del rischio residuo, non sono al momento previste ulteriori misure di sicurezza.

5.3 Opinione del DPO

Il DPO ha espresso un parere in merito al presente documento che è agli atti dell'ufficio privacy e dpo.

6. Fase 7: Eventuale consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR

Dato che il trattamento dei dati personali non rientra nei casi previsti dall'art. 110 del D.lgs 196/2003, il Titolare non procederà alla consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR.

CALCOLO DEL LIVELLO DEL RISCHIO

La seguente valutazione del rischio si basa sulla metodologia sviluppata dell'European Union Agency For Network and Information Security (ENISA) descritta all'interno del documento "Guidelines for SMEs on the security of personal data processing" raggiungibile al seguente link
https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

Response was added on 13.12.2024 16:08.

TITOLO DELLO STUDIO	Predittori per la sepsi ospedaliera. Uno studio di coorte longitudinale del nodo OHDSI italiano" - OMOP_SEPSIS
ACRONIMO DELLO STUDIO	OMOP_SEPSIS
PRINCIPAL INVESTIGATOR	Catherine Klersy

Il livello del rischio viene calcolato moltiplicando il valore dell'Impatto (conseguenze negative per gli Interessati di una determinata minaccia) per la Probabilità che una determinata minaccia si possa verificare.
Pertanto, il livello del rischio è pari a:

LIVELLO DEL RISCHIO = IMPATTO X PROBABILITÀ OCCORRENZA DELLA MINACCIA

CALCOLO DELL'IMPATTO

Il livello d'Impatto deve essere valutato in relazione alle seguenti variabili:

- perdita di riservatezza dei dati;
- perdita d'integrità dei dati;
- perdita di disponibilità dei dati.

Tabella 1

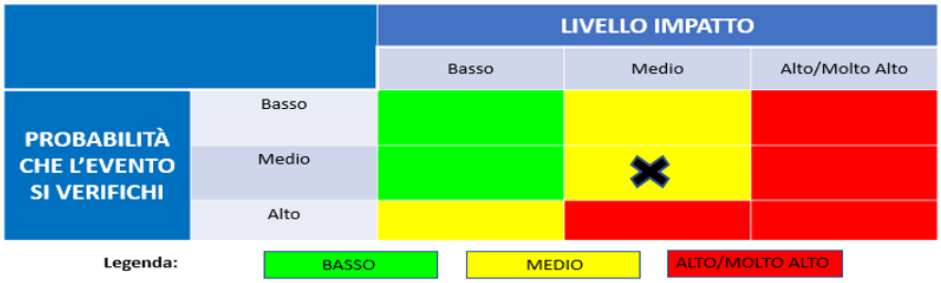
LIVELLO DI IMPATTO	VALORE	DESCRIZIONE
BASSO	1	Gli individui possono andare incontro a **disagi minori**, che supereranno **senza alcun problema** (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
MEDIO	2	Gli individui possono andare incontro a **significativi disagi**, che saranno in grado di superare nonostante **alcune difficoltà** (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
ALTO	3	Gli individui possono andare incontro a **conseguenze significative**, che dovrebbero essere in grado di superare anche se con **gravi difficoltà** (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
MOLTO ALTO	4	Gli individui possono subire **conseguenze significative**, o addirittura irreversibili, **non superabili** (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Si considerano i seguenti livelli di Impatt

LIVELLO FINALE DELL'IMPATTO	**MEDIO**

LIVELLO FINALE DELLA PROBABILITÀ DELLE MINACCE	**MEDIO**

LIVELLO FINALE DEL RISCHIO



LIVELLO DEL RISCHIO	**MEDIO**