ESTRATTO
VALUTAZIONE DI IMPATTO

"STUDIO OSSERVAZIONALE RETROSPETTIVO MULTICENTRICO VOLTO A VALUTARE L'IMPATTO DEL CAMBIO DI TERAPIA INDOTTO SUGLI ESITI CLINICI DELLE INFEZIONI DA MICRORGANISMI PRODUTTORI DI AMPC - SWITCH-AMPC (STUDY ON WHETHER INDUCED THERAPY CHANGE)"

Versione:	***1.0 14/07/2026***

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 centro partecipante, avendone determinato finalità e mezzi di trattamento.
Il Principal Investigator (Responsabile dello studio) è – *omissis*-

1.2 Contesto di riferimento

Oggetto della presente valutazione d'impatto (Data Protection Impact Assessment – DPIA) è il trattamento dei dati personali dei pazienti che saranno arruolati al fine di condurre:

- uno studio clinico osservazionale retrospettivo

Tale studio sarà:

- multicentrico coordinato da altri

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 con la collaborazione del Team Privacy.

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 "*Studio osservazionale retrospettivo multicentrico volto a valutare l'impatto del cambio di terapia indotto sugli esiti clinici delle infezioni da microrganismi produttori di AmpC - SWITCH-AmpC (Study on Whether Induced Therapy Change)*" e documentazione studio specifica.

2.1.2 Ruoli e responsabilità collegate al trattamento.

I soggetti che possono intervenire oltre il Titolare del trattamento sono:

- ASST FATEBENEFRATELLI SACCO – PO Ospedale Luigi Sacco, in qualità di Promotore e Titolare Autonomo del trattamento.

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.

2.1.2.1.1 Persone fisiche che intervengono nel trattamento:

Le persone fisiche e relativi ruoli saranno elencate nel Delegation Log e includono:

Cognome Nome	**Ruolo**
Omissis	Principal Investigator
Omissis	Study Coordinator

2.1.3 Attività di trattamento

Le attività di trattamento sono finalizzate a confrontare l'outcome clinico, ovvero il successo terapeutico (clinical cure) a 8 giorni dall'avvio della terapia antibiotica tra il gruppo 1 (no switch) nel quale la terapia potenzialmente induttrice di AmpC è stata mantenuta e il gruppo 2 (switch) nel quale è stato effettuato uno switch verso un antibiotico stabile all'idrolisi di AmpC.

2.1.4 Ciclo di vita del trattamento dei dati

I dati clinici presenti nelle cartelle cliniche vengono pseudonimizzati e inseriti nella CRF elettronica fornita dal Promotore. Al termine della sperimentazione, la CRF viene validata dal PI e chiusa.

2.1.5 Finalità e obiettivi del trattamento

Le finalità del trattamento sono:

1) Di ricerca scientifica

2.1.6 Categorie di Interessati

2.1.6.1. Categorie di Interessati: pazienti adulti ospedalizzati con diagnosi microbiologicamente confermata di infezione da Enterobacterales AmpC inducibile a rischio moderato, a basso rischio o incerto.

2.1.6.2. Numero indicativo degli interessati coinvolti: 20-76 presso il nostro Centro.

2.1.7 Dati oggetto di trattamento

2.1.7.1. Dati comuni trattati:

- Dati anagrafici: nome, cognome, età, sesso;
- Dati di contatto: indirizzo mail, telefono;

2.1.7.2. Dati appartenenti alle categorie particolari trattati:

- dati personali che rivelino l'origine razziale o etnica
- dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
- Dati contenuti nella CRF: dati relativi al ricovero, dati relativi al decorso dell'infezione (indice di comorbidità di Charlson, dati microbiologici, fonte dell'isolamento, parametri biochimici, parametri clinici, schema terapeutico e outcomes)

2.2 Dati, processi e beni/strumenti di supporto

Si fa riferimento al protocollo di studio e documentazione studio specifica;

Beni di supporto
I beni di supporto possono essere raggruppati in:

- Fonti dei dati:

o Cartelle cliniche

- Software per la gestione della CRF (e-CRF): sistema per la gestione eCRF, applicativo web fornito dal Promotore.

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

3.1 Proporzionalità e necessità

Lo scopo di miglioramento del processo di cura/prevenzione attraverso la ricerca clinica 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 Fondamenti legali del trattamento

La base giuridica del trattamento si fonda su:

- Art. 110 d.lgs. 196/2003 (valutazione d'impatto ai sensi dell'art. 35 del GDPR e applicazione di misure a garanzia ai sensi dell'art. 106, comma 2, lettera d).

Nel caso di specie, per la fase retrospettiva, per alcuni o per la totalità degli interessati non è possibile acquisire il consenso in quanto

a) non contattabili o deceduti;

- Consenso dell'interessato ex art. 6, par.1 lett. a) e art. 9, par. 2, lett. a) del GDPR.

Il consenso è:
- liberamente conferito: la scelta di partecipare allo studio è opzionale e facoltativa, in quanto non l'interessato non subisce conseguenze negative in termini di assistenza sanitaria ricevuta.
- specifico: il consenso viene richiesto per ogni specifica finalità che lo prevede.
- informato: all'interessato sono fornite le opportune informazioni ai sensi degli artt. 12-13 del GDPR.
- inequivocabile: il consenso viene prestato attraverso l'apposizione di firma quale azione positiva dell'utente
- esplicito: la richiesta di consenso è costruita in moda tale da presentare all'utente sia l'opzione di acconsentire sia l'opzione di non acconsentire al trattamento
- revocabile in qualsiasi momento: l'interessato può esercitare il diritto di revoca tramite richiesta effettuata al Titolare del trattamento nella persona del Responsabile dello studio

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

Per l'esecuzione del trattamento, il Titolare del trattamento raccoglierà solo i dati adeguati, rilevanti e limitati a quanto necessario per il conseguimento delle finalità del trattamento. Si rimanda a tal fine alla procedura aziendale e al Protocollo di studio.

3.1.3 Accuratezza ed aggiornamento dei dati

Gli Sperimentatori verificano la correttezza dei dati raccolti sulla scheda raccolta dati confrontandoli con quelli presenti sulla cartella clinica del partecipante. 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 (cartella clinica) 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. La chiave per risalire all'oggetto sarà conosciuta solo dal Principal Investigator e dai ricercatori del gruppo di ricerca autorizzati dal PI.
I dati raccolti saranno oggetto di un'attività di anonimizzazione, sulla base del WP 216 5/2014 per la pubblicazione e alla fine dello studio.

3.1.4 Durata della conservazione dei dati

I Dati personali dell'interessato saranno conservati per il solo tempo necessario ai fini per cui sono stati raccolti, rispettando i principi di limitazione della conservazione e minimizzazione definiti nell'art. 5 del GDPR.
I Dati saranno custoditi per conformarsi agli obblighi regolatori e perseguire le finalità del trattamento, in conformità coi principi di necessità, minimizzazione e adeguatezza.
Il Titolare del trattamento dichiara che i dati personali dell'interessato oggetto di trattamento saranno conservati per 1 anno, come specificato nel protocollo e nell'informativa specifica dello studio.

3.2 Controlli per proteggere i diritti degli interessati

3.2.1 Come sono informati gli interessati circa il trattamento

Si rimanda all'informativa al trattamento dei dati personali studio-specifica pubblicata sul sito internet.

3.2.2 Esercizio dei diritti da parte degli interessati

Si rimanda alla procedura aziendale disponibile sul sito intranet:
https://intranet.sanmatteo.org/documenti/io-06504-esercizio-diritti-interessati-ambito-privacy

Si rimanda a vademecum per gli utenti disponibile sul sito internet alla sezione privacy: https://www.sanmatteo.org/privacy

3.2.3 Obbligazioni dei responsabili del trattamento

Non risultano responsabili esterni del trattamento per la Fondazione.

3.3 Trasferimenti al di fuori dello SEE

I suoi dati personali **non** verranno trasferiti fuori dall'Unione Europea.

Il Promotore potrà comunicare i dati personali verso altre affiliate del gruppo del Promotore e verso terzi operanti per suo conto, compresi quelli all'estero, in paesi extra UE che non offrono lo stesso livello di protezione dei dati garantito dal Regolamento UE 2016/679. In tal caso sarà onere del Promotore, quale Titolare autonomo del trattamento dei Suoi dati, adottare e far adottare ai propri affiliati e terzi soggetti nello svolgimento delle attività dello Studio, tutte le misure necessarie a garantire un adeguato e sufficiente livello di protezione dei dati, in applicazione degli articoli 44, 45, 46, 47, 48, 49, 50 del Regolamento UE 2016/679; l'Interessato potrà contattare il Promotore, anche tramite la Fondazione (in persona del Medico sperimentatore che lo segue per assicurare la riservatezza della sua identità), al fine di richiedere tutte le informazioni relative al predetto trattamento di dati.

4. Fase 3: Calcolo del livello del rischio

Il livello del rischio e le relative misure di mitigazione viene calcolato utilizzando l'allegato "ADDENDUM CALCOLO DEL RISCHIO".

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

L'indice di questo documento e relativi contenuti rispecchiano quanto indicato nell'allegato 2 del WP 248 *(Criteri per una valutazione d'impatto sulla protezione dei dati accettabile)* (cfr. Comitato Europeo per la protezione dei dati, Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248rev.01).
Il DPO, consultato dal Titolare in conformità all'art. 35, par. 2, del GDPR in merito alla Valutazione d'impatto ex artt. 35-36 GDPR (cd. DPIA) sulle attività di trattamento relative allo "*Studio osservazionale retrospettivo multicentrico volto a valutare l'impatto del cambio di terapia indotto sugli esiti clinici delle infezioni da microrganismi produttori di AmpC" - SWITCH-AmpC (Study on Whether Induced Therapy Change)"* nello svolgimento dei compiti attribuitigli, ha valutato che**:**

Cfr. parere DPO

VALUTAZIONE DI IMPATTO

Addendum a DPIA quale parte integrante formale e sostanziale.

1 Rispetto dei principi di Privacy by Design e calcolo dell'Impatto

1.1 Software per la gestione della CRF (e-CRF) e Infrastruttura

- *- omissis -* .

- Infrastruttura:
  - Computer dedicato,
  - *- omissis*
  - Rete: collegamento da Intranet aziendale, e connessione protetta da rete pubblica

Rispetto delle strategie

1. Minimizzare: sono trattati soltanto i dati necessari per raggiungere le finalità
2. Aggregare: sono applicate misure di pseudonimizzazione che prevedono tale strategia
3. Nascondere: il trattamento dei dati personali è limitato soltanto a soggetti autorizzati ed i dati vengono conservati in forma cifrata
4. Informare: all'interessato sono fornite tutte le informazioni pertinenti al trattamento in oggetto (informative ex artt. 13 e 14 GDPR)
5. Controllare: all'interessato è garantito l'esercizio dei diritti previsti dalla normativa (artt. 15-22 GDPR). Si rinvia alla procedura di gestione dei diritti degli interessati.
6. Dimostrare: si rinvia alle policy del Titolare del trattamento

2 Calcolo dell'impatto

Si considerano i seguenti livelli di Impatto:

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.).

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.

-omissis –

3 Calcolo del livello di rischio

Il livello del rischio sarà dato dalla moltiplicazione del risultato del livello d'impatto per il risultato del livello di probabilità.

LIVELLO DEL RISCHIO	**ALTO**

4 Individuazione delle misure che mitigano il rischio

Determinato il livello del rischio, e individuate le minacce e le fonti che potrebbero concretizzarlo, vengono individuate ora le misure di sicurezza che contribuiscono alla mitigazione del rischio stesso.

Perdita di riservatezza

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Le principali minacce relative alla perdita di riservatezza riguardano comportamenti umani quali, ad esempio, condivisione dei dati personali con soggetti non autorizzati, errori nelle configurazioni di sicurezza del PC che permettendo accessi illegittimi, attacchi informatici esterni, violazione di account.

Quali sono le fonti di rischio?

Le fonti di rischio sono quindi costituite principalmente da operatori interni mal istruiti o insoddisfatti, attacchi esterni tramite phishing, social engineering o sfruttamento di vulnerabilità.

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità di accadimento delle minacce?

La probabilità di accadimento delle minacce è mitigata da diverse misure che verranno descritte nel dettaglio nel paragrafo 6. In particolare, le misure che maggiormente contribuisco a garantire una maggior tutela della riservatezza sono la pseudonimizzazione, la prevenzione del malware, la MFA e la segmentazione di rete.

- I dati contenuti nella Base Dati sono infatti pseudonimizzati e non permettono quindi di risalire

direttamente all'identità degli Interessati.
- *- omissis*
- Gli accessi fisici sono controllati e le postazioni gestite.
- Viene erogata regolare formazione agli autorizzati al trattamento.
- Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, crittografia, gestione del personale, vulnerabilità.

Perdita d'integrità
Quali sono le principali minacce che potrebbero concretizzare il rischio?

Le principali minacce relative alla perdita di integrità riguardano ridotti controlli di qualità sulle procedure di data entry. L'errore più probabile potrebbe essere un errore nel mappaggio tra il dato originale e la codifica standard di riferimento. I rischi potrebbero, inoltre, concretizzarsi a seguito di attacchi informatici ed errori umani.

Quali sono le fonti di rischio?

Le fonti di rischio principali riguardano: un operatore interno mal istruito o insoddisfatto, attaccante esterno tramite phishing, social Engineering o sfruttamento di vulnerabilità.

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

Le misure, meglio descritte nel paragrafo 6, adottate per mitigare i rischi di perdita d'integrità sono le seguenti
- Prima di tutto vengono eseguiti diversi controlli di qualità sui dai (descritti alla sezione 3.1.2.5) che ne garantiscono l'integrità
- *- omissis*
- Gli accessi fisici sono controllati e le postazioni gestite.
- Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, crittografia, vulnerabilità.

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

La principale minaccia relativa alla perdita di disponibilità riguarda la distruzione accidentale della Base Dati o fisica del server.

Quali sono le fonti di rischio?

Le fonti di rischio per una perdita di disponibilità sono: attività volontaria di un operatore interno con accesso alla Base Dati; attaccante esterno tramite phishing, social Engineering o sfruttamento di vulnerabilità. Errore umano interno per disattenzione/incompetenza. Perdita della password.

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

Le misure adottate per mitigare la perdita di disponibilità dei dati, meglio descritte nel paragrafo 6, riguardano principalmente la presenza di un backup - *omissis* Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici e degli accessi fisici, archiviazione, partizionamento, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, vulnerabilità, lotta contro il malware, gestione postazioni, gestione dei rischi, gestione del personale, sicurezza dei canali informatici, sicurezza dell'hardware e vigilanza sulla protezione dei dati.

5. Misure di mitigazione adottate

5.1 Crittografia – Cifratura

Vengono implementate le seguenti tecniche di cifratura dei dati personali:
- *omissis* –

5.2 Pseudonimizzazione

Vengono implementate tecniche di pseudonimizzazione, al fine di ottenere la separazione tra i dati identificativi del paziente e i dati della eCRF

- *omissis* -
Il responsabile dei dati e della loro pseudonimizzazione è lo sperimentatore principale.

5.3 Controllo degli accessi logici

L'accesso alla eCRF tramite l'applicativo - *omissis* -

5.4 Tracciabilità

La Piattaforma – *omissis* - è dotata di una applicazione – *omissis* -, tramite cui vengono registrate tutte le variazioni al progetto,
– *omissis* –

5.5 Minimizzazione dei dati

Verranno raccolti tutti e soli i dati necessari per rispondere ai quesiti dello studio.

- Le fasi di progettazione dello studio ha implicato il rispetto del principio di minimizzazione
- Lo sperimentatore garantisce che i dati previsti nella CRF sono i soli indispensabili alla conduzione dello studio
- L'esperto statistico garantisce che il numero di interessati è il minimo per dare rilievo allo studio.

5.6 Lotta contro il malware

La Piattaforma – *omissis* - viene aggiornata all'ultima versione rilasciata stabile e sicura disponibile. Tale aggiornamento è demandato ad un Fornitore esterno.
– *omissis* -

5.7 Vulnerabilità

Viene assicurata la protezione contro le vulnerabilità attraverso l'attuazione di una manutenzione ordinaria dei sistemi aziendali per l'applicazione di patch di sicurezza.
– *omissis* –

5.8 Backup

Il Titolare è responsabile delle procedure di backup a livello di virtualizzazione o, copia periodica del server database sono impostati backup giornalieri, mensili ed annuali e retention – *omissis* -.

5.9 Archiviazione

I dati vengono conservati sui server del Titolare fino a – *omissis* - successivi al termine dello studio. Il personale autorizzato della Direzione Scientifica si occupa della gestione degli accessi e recupero delle password.
– *omissis* -

5.10 Sicurezza dei documenti cartacei

Le configurazioni di sicurezza relative all'hardware su ci è installata la Piattaforma sono demandate al personale IT del Titolare.
I documenti cartacei prodotti dallo studio sono: documentazione relativa allo studio: il Protocollo, la sinossi, la CRF, il consenso sanitario ecc., i moduli dell'informativa e del consenso al trattamento dei dati personali ai sensi dell'art. 13 del Regolamento UE 679/2016- GDPR, cartelle ambulatoriali.
Essi sono conservati in armadi chiusi a chiave ed in locali dotati di misure antincendio – *omissis* -.

5.11 Sicurezza dell'hardware

Il computer sarà su dominio locale e disporrà delle ultime patch di sicurezza sempre aggiornate e adeguate alle ultime indicazioni di buona pratica.
Sono applicate le opportune configurazioni di sicurezza relative all'hardware.

5.12 Gestione postazioni

Il Titolare gestisce le proprie postazioni con XDR.
La gestione delle postazioni comprende la postazione di lavoro dedicata – *omissis* -.
Al computer dedicato per le attività avranno accesso solo il Data Manager e il responsabile scientifico del progetto.
Il computer resterà acceso solo durante il suo utilizzo.

– omissis –

5.13 Manutenzione

La manutenzione del server fisico è demandata al personale IT del Titolare e al fornitore appositamente incaricato e nominato e sono applicate le patch e gli aggiornamenti periodici (O.S.) rilasciati dalla casa madre.
Il personale del Fornitore esterno è responsabile del piano di manutenzione ordinaria ed eventualmente evolutiva della Piattaforma – *omissis* -. Il Fornitore esterno esegue un aggiornamento annuale del sistema a versioni compatibili.

5.14 Contratto con il responsabile del trattamento

Il contratto con i responsabili del trattamento contiene opportune istruzioni e disciplina i rispettivi obblighi per assicurare la protezione dei dati personali.

5.15 Controllo degli accessi fisici

Il Titolare ha previsto un protocollo di controllo degli accessi fisici ai locali che ospitano i server – *omissis* -.

5.16 Protezione contro fonti di rischio non umane

Protezione contro fonti di rischio non umane: La presenza di backup giornalieri, mensili ed annuali e retention – *omissis* -.
Eventuali altri controlli legati a guasti, difetti dell'architettura IT, alimentazione, rischi ambientali sono demandati al Titolare.

5.17 Politica di tutela della privacy

Le politiche privacy del Titolare del trattamento e dei responsabili del trattamento, relative alla propria organizzazione, sono conformi al GDPR.
Il DPO di Fondazione IRCCS Policlinico San Matteo ha un ruolo di verifica dei trattamenti nei confronti del Titolare del trattamento dati
È stato emesso un Organigramma Privacy che definisce i ruoli all'interno dell'azienda e sono state definite le procedure per la gestione dei diritti degli interessati e la gestione delle violazioni di dati personali.

5.18 Gestione dei rischi

È stata effettuata la valutazione dei rischi i cui risultati sono nello specifico paragrafo.

5.19 Integrare la protezione della privacy nei progetti

La fase di progettazione ha tenuto conto dei requisiti di privacy by design.

5.20 Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Il Titolare ha adottato una procedura per la gestione degli incidenti di sicurezza.
Gli accordi in essere prevedono la collaborazione di tutti gli Enti coinvolti in caso di incidente.

5.21 Gestione del personale

Il Titolare ha provveduto ad autorizzare il personale a vario titolo coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati).

Inoltre, ha provveduto a comunicare la disponibilità di procedure privacy al personale a vario titolo coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati). Le Procedure sono reperibili sulla intranet aziendale.
Sono state svolte attività di formazione (formazione residenziale e corsi FAD) per tutto il personale che a vario titolo è coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati). Inoltre, pianifica annualmente gli interventi formativi.

5.22 Gestione dei terzi che accedono ai dati

Il CET potrà eventualmente accedere ai dati nello svolgimento dei suoi compiti istituzionali. I dati potranno essere richiesti in via teorica sulla base del L.241/90 da specifici portatori di interesse e con le relative cautele normativamente previste.

5.23 Vigilanza sulla protezione dei dati

Il Titolare ha nominato un DPO con il compito di vigilare sui trattamenti dei dati personali.

6 Opinione del DPO

Cfr. parere DPO

7 Monitoraggio e riesame nel tempo della DPIA

Ai sensi del paragrafo 11 dell'art. 35 del GDPR, il Titolare deve:

- verificare che il trattamento dei dati personali sia effettuato conformemente alla DPIA. A tal fine il DPO effettuerà degli audit con cadenza annuale;
- procedere a un riesame del trattamento oggetto di DPIA quando vengono apportate modifiche al trattamento con conseguente variazione del livello di rischio connesso al trattamento stesso, al fine di valutare la necessità di apportare revisioni al DPIA Report ovvero di effettuare una nuova DPIA.

Per valutare se il livello di rischio è variato, si dovrà verificare se sono stati modificati uno o più dei seguenti aspetti:

- Cambiamento sulle attività di trattamento, in termini di:
  - contesto (variazione della localizzazione fisica o di elementi ambientali dell'azienda, nuovi vincoli, funzioni e struttura organizzativa, innesto di politiche e processi aziendali, leggi, norme e contratti);
  - modalità di raccolta dei dati personali (mediante modulo cartaceo o form elettronico, direttamente dall'interessato o indirettamente da terzi)
  - finalità del trattamento;
  - tipologia di dati personali trattati (ad esempio dati genetici);
  - categorie di interessati;
  - soggetti coinvolti nel trattamento (personale interno all'organizzazione o fornitori esterni);
  - combinazioni di dati (integrazione con dati provenienti da altre sorgenti, correlazione di informazioni censite su diverse basi dati);
  - trasferimento di dati all'estero (all'interno della UE o verso paesi od organizzazioni internazionali al di fuori della UE).
- Modifica ai rischi con impatti sui diritti e le libertà delle persone fisiche, derivanti da:
  - Modifica dei sistemi informativi a supporto (subentro di un nuovo Service Provider, migrazione di servizi in Cloud, ecc.);
  - nuovi scenari di rischio (furti di identità e frodi informatiche, introduzioni di attacchi avanzati e azioni non autorizzate)
  - insorgenza di potenziali impatti sulle qualità di riservatezza, integrità e disponibilità dei dati personali;
  - nuove minacce (naturali, ambientali, tecniche, di terrorismo o sabotaggio, provenienti da comportamenti volontari o accidentali);

- attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali;
- dismissione di elementi di presidio esistenti.

- Mutamenti nel contesto organizzativo o sociale per l'attività di trattamento, ad esempio perché gli effetti di determinate decisioni automatizzate sono diventati più significativi oppure perché nuove categorie di interessati sono diventati vulnerabili alla discriminazione.

A seguito delle predette verifiche dovrà essere calcolato il livello di rischio (utilizzando la procedura di cui al punto 7) e acquisito il parere del DPO in merito alla necessità di aggiornare la DPIA ovvero procedere ad una nuova valutazione d'impatto.
In ogni caso, anche a prescindere da modifiche apportate al trattamento, quest'ultimo sarà oggetto di riesame annuale, al fine di verificate se, a seguito di cambiamenti nelle conoscenze tecnico-scientifiche, si sia modificato il livello di rischio e sia quindi necessario adottare misure tecnico organizzative nonché rivedere/integrare la DPIA al fine di mantenere la validità e l'aggiornamento nel tempo della valutazione condotta e dei suoi risultati.