



Nome del DPO/RPD

Giuseppe Mercurio

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

Considerate le misure di minimizzazione del trattamento dei dati e le modalità di archiviazione degli stessi; considerate le misure di sicurezza dei canali informatici e le politiche di tutela della privacy, nonché la gestione degli incidenti di sicurezza e violazione dei dati personali, il rischio della perdita del controllo dei dati e della violazione della riservatezza residuo risulta trascurabile.

Pertanto il trattamento può essere implementato.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Viste le misure pianificate e/o esistenti, pur considerando l'importanza dei rischi, vi è una probabilità trascurabile che tali rischi si verifichino.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento considerato è quello relativo al progetto MedWriter finanziato dal Ministero delle imprese e del Made in Italy (Fondo per la crescita sostenibile - Scoperta Imprenditoriale) per il quale la Fondazione di Religione e di Culto Casa Sollievo della Sofferenza - Opera di San Pio da Pietrelcina, IRCCS (di seguito, nella presente DPIA, anche "Fondazione"), ha stipulato un contratto con il capofila Fiven S.p.A. in data 14/10/2025 (rif. PROGETTO "MEDWRITER – SOLUZIONE AI PER LA GESTIONE EFFICIENTE DEI PAZIENTI NEI REPARTI OSPEDALIERI", COD. PROG. F/360172/00/X75 CUP: B69J24000580005).

Il progetto ha come obiettivo l'utilizzo di metodologie e strumenti di intelligenza artificiale per la costruzione di bozze di report clinici (es. lettere di dimissione, note cliniche ecc.) sulla base di dati

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-PR-8-DPIA-MEDWRITER	00	13/01/2026	UOC INNOVAZIONE E INTELLIGENZA ARTIFICIALE AI UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	1 di 11



strutturati presenti nei record dei pazienti in carico alla Fondazione e presenti sul sistema informativo sanitario aziendale SISWeb.

Le bozze elaborate non avranno un effetto sulle cure prestate ai pazienti dai professionisti sanitari della Fondazione in quanto i tool sviluppati nel progetto hanno esclusivamente finalità di facilitazione redazionale dei documenti clinici.

Il trattamento avverrà per una duplice finalità:

- 1) addestramento di un Large Language Model (LLM) ospitato all'interno del perimetro della rete ospedaliera;
- 2) creazione, a partire dai dati clinici dei pazienti, delle rispettive bozze di documenti clinici.

I tool sviluppati dal progetto non determineranno alcun impatto in merito alla attribuibilità dei documenti ai professionisti medici che hanno in carico i pazienti a cui i documenti di riferiscono. Gli stessi professionisti, come da normative applicabili, continueranno a detenere l'onere di sottoscrivere (digitalmente o in altre modalità consentite) i documenti clinici.

Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento dei dati è la Fondazione di Religione e di Culto Casa Sollievo della Sofferenza - Opera di San Pio da Pietrelcina, IRCCS.

In virtù del citato rapporto contrattuale di fornitura di servizi di ricerca, l'azienda Fiven S.p.A. verrà nominata Responsabile del Trattamento ex Art. 28 GDPR prima dell'inizio del trattamento dei dati personali.

Ci sono standard applicabili al trattamento?

Il Titolare del Trattamento adotta uno standard UNI EN ISO 9001:2015 (Sistema di Gestione della Qualità) e uno standard UNI CEI ISO/IEC 27001:2013 (Sistema di Gestione della Sicurezza delle Informazioni).

Tutte le misure da implementare saranno in linea con quanto previsto dal Regolamento (UE) 2016/679 ("GDPR"), dal Regolamento (UE) 2024/1689 ("AI Act") e dalla Legge 132/2025.

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-PR-8-DPIA-MEDWRITER	00	13/01/2026	UOC INNOVAZIONE E INTELLIGENZA ARTIFICIALE AI UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	2 di 11



I dati oggetto del trattamento sono tutti quelli presenti sul sistema informativo sanitario SISWeb, adottato dalla Fondazione di Religione e di Culto Casa Sollievo della Sofferenza - Opera di San Pio da Pietrelcina, IRCCS per la gestione digitalizzata dei dati dei pazienti in carico ad essa per finalità di cura.

I dati comprendono:

- Anagrafica dei pazienti;
- Condizioni cliniche dei pazienti risultati dagli esami effettuati all'interno dell'ente (esami di laboratorio, esami radiologici, cardiologici, di anatomia patologica, consulenze specialistiche e più in generale, tutti gli esami clinici effettuati all'interno della struttura che esitano nella produzione di un risultato o referto in versione digitale integrato all'interno del sistema SISWeb);
- Farmaci somministrati ai pazienti;
- Percorso dei pazienti in ospedale per ricovero (Accettazioni-Dimissioni-Trasferimenti) e/o per accessi ambulatoriali.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Addestramento LLM con accesso ai dati strutturati del database SISWeb e alla documentazione clinica risultate dell'episodio di ricovero.

Utilizzo del LLM (inferenza - RAG) sul quale si è effettuato l'addestramento per la generazione della bozza di documento clinico.

Il modello LLM addestrato sui dati della Fondazione non sarà utilizzato da Fiven per alcuna altra finalità differente da quelle previste nel progetto MedWriter **Quali sono le risorse di supporto ai dati?**

I dati presenti sul sistema informativo SISWeb sono attualmente ospitati on premises presso la infrastruttura tecnologica della Fondazione secondo elevati standard di sicurezza dettati dalla normativa e dalle procedure di interne di conformità alla norma ISO 27001.

Il LLM che sarà utilizzato per il progetto risiederà fisicamente presso la infrastruttura tecnologica della Fondazione e sarà dotato di collegamento verso reti esterne esclusivamente attraverso una VPN (Virtual Private Network) necessaria a Fiven per l'accesso remoto al sistema per finalità di configurazione, manutenzione e fine-tuning.

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-PR-8-DPIA-MEDWRITER	00	13/01/2026	UOC INNOVAZIONE E INTELLIGENZA ARTIFICIALE AI UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	3 di 11



Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati personali raccolti nell'ambito degli studi generati dal progetto MedWriter saranno trattati esclusivamente per le finalità indicate nel contratto stipulato dalla Fondazione con Fiven, nonché indicate nei documenti di progetto. Di seguito, per completezza, le finalità del trattamento:

- Progettazione di algoritmi per l'estrazione ed analisi dei dati e la generazione delle lettere di dimissione;
- Progettazione di algoritmi per la creazione di specifici Clinical Decision Support Systems (CDSSs) orientati sia alla fase diagnostica che terapeutica.

Si ottempera, in ogni caso, al "principio di limitazione della finalità", per il quale i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

Quali sono le basi giuridiche che rendono lecito il trattamento?

La base giuridica per il trattamento dei dati, oggetto della presente DPIA, è costituita dal "rilevante interesse pubblico" ex Art. 9.2 lett. g) del Regolamento (UE) 2016/679, in attuazione dei disposti di cui all'Art. 8 della L. 132/2025.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti sono adeguati per le finalità del progetto MedWriter in quanto si riferiscono a pazienti in carico alla struttura per attività di ricovero o ambulatoriali, per vengono routinariamente prodotte note cliniche sotto forma di testo non strutturato.

I dati sono esatti e aggiornati?

I dati sono esatti entro i limiti di accuratezza associati alle possibilità degli operatori sanitari che li immettono nel sistema informativo sanitario e/o alla accuratezza strumentale dei dispositivi medici che generano i dati che sono presenti sul sistema informativo.

I dati sono aggiornati in quanto ogni variazione degli stessi viene riportata dai professionisti sanitari sui sistemi.

Qual è il periodo di conservazione dei dati?

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-PR-8-DPIA-MEDWRITER	00	13/01/2026	UOC INNOVAZIONE E INTELLIGENZA ARTIFICIALE AI UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	4 di 11



I dati generati dal progetto (bozze di note cliniche) saranno conservati per un periodo di 10 anni a partire dalla loro generazione (presumibilmente: marzo 2026), anche nell'ottica della generazione di dati aggregati utili al fine di produrre pubblicazioni scientifiche nel breve/medio e lungo termine.

Principi Fondamentali

Misure a tutela dei diritti degli interessati Come

sono informati del trattamento gli interessati?

Gli interessati saranno informati mediante apposite informazioni ex Art. 13 o 14 GDPR da pubblicare, a cura della Fondazione, sul Portale "<https://operapadrepio.it/>" prima dell'inizio del trattamento dei dati.

Ove applicabile: come si ottiene il consenso degli interessati?

Non applicabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

L'esercizio dei diritti da parte degli interessati potrà avvenire mediante le informazioni ex Art. 13 o 14 GDPR da pubblicare, a cura della Fondazione, sul Portale "<https://operapadrepio.it/>" prima dell'inizio del trattamento dei dati.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

L'esercizio dei diritti da parte degli interessati potrà avvenire mediante le informazioni ex Art. 13 o 14 GDPR da pubblicare, a cura della Fondazione, sul Portale "<https://operapadrepio.it/>" prima dell'inizio del trattamento dei dati.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

L'esercizio dei diritti da parte degli interessati potrà avvenire mediante le informazioni ex Art. 13 o 14 GDPR da pubblicare, a cura della Fondazione, sul Portale "<https://operapadrepio.it/>" prima dell'inizio del trattamento dei dati.

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-PR-8-DPIA-MEDWRITER	00	13/01/2026	UOC INNOVAZIONE E INTELLIGENZA ARTIFICIALE AI UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	5 di 11



Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Gli obblighi del Responsabile del Trattamento saranno identificati nell'atto di nomina che verrà stipulato secondo il modello delle SCC (Standard Contractual Clauses).

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati non verranno trasferiti al di fuori dell'Unione Europea.

Rischi

Misure esistenti o pianificate

Minimizzazione dei dati

Al fine di ridurre il rischio, nell'ambito progettuale viene memorizzato soltanto il set minimo delle informazioni necessarie all'esecuzione delle attività di sperimentazione.

Controllo degli accessi logici

Gli accessi ai sistemi sono definiti utilizzando il principio dei "Privilegi Minimi" necessari allo svolgimento delle operazioni e avvengono tramite una coppia "nome utente" e "password" definita per ogni utente autorizzato alla consultazione dei dati. L'accesso ai server è garantito, grazie all'impiego di un firewall. Relativamente alle connessioni da rete interna, essa è possibile esclusivamente da postazioni appartenenti al dominio della Fondazione e dagli utenti autorizzati all'accesso

Back-up

Viene eseguita una copia di backup locale dei dati presenti sul sistema Fiven installato presso la Fondazione. Nello specifico, viene effettuata una copia di sicurezza delle bozze delle lettere di dimissioni generate dall'applicativo, al fine di prevenire eventuali perdite di dati che comporterebbero un significativo impegno operativo per la riconfigurazione del sistema. Tale backup è finalizzato esclusivamente a garantire il corretto funzionamento degli applicativi.

Security Operation Center ospedaliero

Il SOC aziendale è operativo secondo le procedure specificate alla luce della certificazione aziendale secondo la norma ISO 27001.

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-PR-8-DPIA-MEDWRITER	00	13/01/2026	UOC INNOVAZIONE E INTELLIGENZA ARTIFICIALE AI UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	6 di 11



Crittografia

La crittografia dei dati durante il transito dalla rete interna della Fondazione verso postazioni esterne della rete Fiven è garantito dall'utilizzo di una connessione cifrata VPN. I dati della rete interna della Fondazione non sono sottoposti ad azioni crittografiche.

Controllo degli accessi fisici

I dati memorizzati risiedono su server interni al perimetro della rete della Fondazione ed ospitati all'interno della server farm aziendale.

Restrizioni nella modifica dei dati

Verrà impostato l'accesso in sola lettura come unica tipologica di accesso possibile da parte dei server di Fiven verso i server aziendali della Fondazione.

Rischi

Accesso illegittimo ai dati

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

Diffusione illegittima di informazioni sullo stato di salute dei pazienti.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Data Breach su sistema informativo ospedaliero, Rottura o malfunzionamento di dispositivi hardware o di software, Attacchi cryptolocker.

Quali sono le fonti di rischio?

Violazione di credenziali, Attacco cyberinformatico.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Security Operation Center ospedaliero, Controllo degli accessi logici, Controllo degli accessi fisici.

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

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-PR-8-DPIA-MEDWRITER	00	13/01/2026	UOC INNOVAZIONE E INTELLIGENZA ARTIFICIALE AI UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	7 di 11



Importante.

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

Trascurabile.

Rischi

Modifiche indesiderate dei dati

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

Modifica di informazioni clinicamente rilevanti per la cura del paziente.

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

Data Breach su sistema informativo ospedaliero, Rottura o malfunzionamento di dispositivi hardware o di software, Attacchi cryptolocker.

Quali sono le fonti di rischio?

Violazione di credenziali, Attacco cyberinformatico.

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

Controllo degli accessi logici, Restrizioni nella modifica dei dati.

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

Importante.

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

Trascurabile, L'accesso ai server aziendali avverrà in modalità esclusiva di sola lettura.

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-PR-8-DPIA-MEDWRITER	00	13/01/2026	UOC INNOVAZIONE E INTELLIGENZA ARTIFICIALE AI UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	8 di 11



Rischi

Perdita di dati

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

Mancanza di informazioni necessarie alla cura dei pazienti.

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

Data Breach su sistema informativo ospedaliero, Rottura o malfunzionamento di dispositivi hardware o di software, Attacchi cryptolocker.

Quali sono le fonti di rischio?

Attacco cyberinformatico, Malfunzionamento software o hardware.

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

Controllo degli accessi logici, Back-up, Security Operation Center ospedaliero, Controllo degli accessi fisici, Restrizioni nella modifica dei dati.

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

Importante.

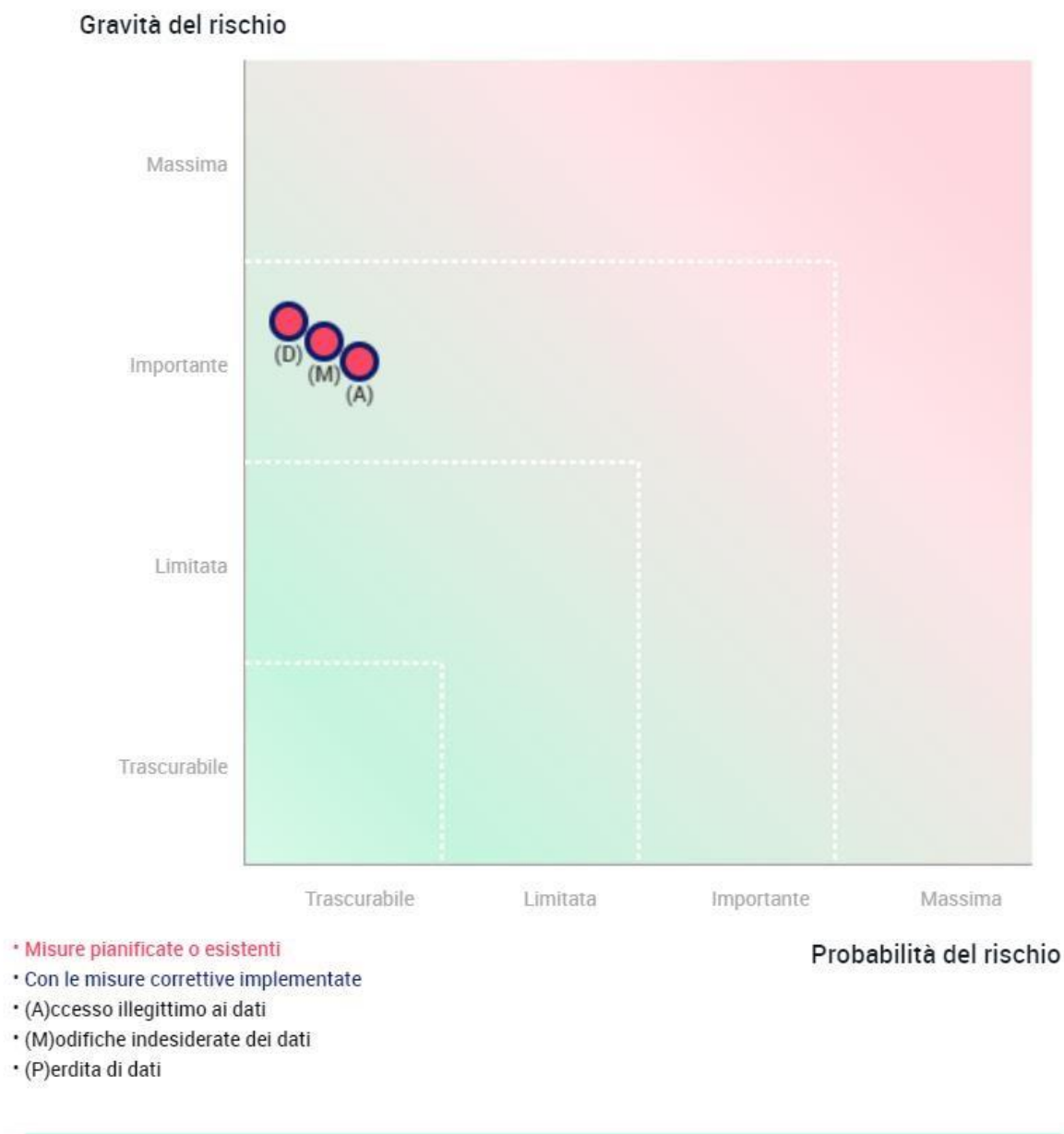
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile.

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-PR-8-DPIA-MEDWRITER	00	13/01/2026	UOC INNOVAZIONE E INTELLIGENZA ARTIFICIALE AI UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	9 di 11



Rischi



28/11/25

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-PR-8-DPIA-MEDWRITER	00	13/01/2026	UOC INNOVAZIONE E INTELLIGENZA ARTIFICIALE AI UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	10 di 11



Impatti potenziali

Diffusione illegittima di i...
Modifica di informazioni c...
Mancanza di informazioni i...

Minaccia

Data Breach su sistema info

Fonti

Violazione di credenziali
Attacco cyberinformatico
Malfunzionamento softwar

Misure

Security Operation Center c...
Controllo degli accessi log...
Controllo degli accessi fis...
Restrizioni nella modifica...
Back-up

Accesso illegittimo ai dati

Gravità : Importante

Probabilità : Trascurabile

Modifiche indesiderate dei dati

Gravità : Importante

Probabilità : Trascurabile

Perdita di dati

Gravità : Importante

Probabilità : Trascurabile

Codice Documento	Revisione	Data Emissione	Emesso	N. Ro Pagina
MO-PR-8-DPIA-MEDWRITER	00	13/01/2026	UOC INNOVAZIONE E INTELLIGENZA ARTIFICIALE AI UO AFFARI GENERALI, LEGALE, CONTRATTI E TUTELA DELLA PRIVACY	11 di 11