

Informazioni sulla PIA

Nome della PIA Valutazione di impatto : Studio 2024MED105 “Esiti clinici nei pazienti ricoverati in reparti di Medicina Interna e adeguatamente trattati per setticemia da *Klebsiella pneumoniae* produttrice di NDM. Uno studio multicentrico retrospettivo nella vita reale in un'area endemica”

Nome autore: Dott. SIMONE MEINI-Direttore delegato UOC Medicina Interna
Responsabile UOS P.I.C.U.
Ospedale F.Lotti Pontedera - ATNO

Nome valutatore: Dott. SIMONE MEINI-Direttore delegato UOC Medicina Interna
Responsabile UOS P.I.C.U.Ospedale F.Lotti Pontedera - ATNO (sentito il parere del DPO aziendale)

Nome validatore : Dott. SIMONE MEINI-Direttore delegato UOC Medicina Interna
Responsabile UOS P.I.C.U. Ospedale F.Lotti Pontedera – ATNO

Data di creazione 23 settembre 2024

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Raccolta retrospettiva relativa agli anni 2021-2022 che include tutti i pazienti ricoverati nelle tre Medicine di Pontedera, Livorno e Versilia per setticemia da *K.pneumoniae* NDM trattati con la terapia migliore possibile, al fine di valutarne la mortalità a 1 mese (dato non noto in letteratura sui pazienti con multimorbilità ricoverati in Medicina).

Quali sono le responsabilità connesse al trattamento?

Doveri di liceità, correttezza, trasparenza e minimizzazione.

Ci sono standard applicabili al trattamento?

DDL n. 1110 di conversione in legge, con modificazioni, del D.L. n. 19/2024, recante ulteriori disposizioni urgenti per l'attuazione del piano nazionale di ripresa e resilienza (PNRR), con il quale, attraverso l'aggiunta del comma 1-bis all'art. 44 del D.L. 19/2024, è stato modificato anche l'art. 110 del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2008 (“Codice Privacy”)

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Dati aggregati di mortalità e caratteristiche comuni demografiche quali età, sesso, comorbidità.

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

6 mesi

Quali sono le risorse di supporto ai dati?

Creazione di file Excel conservato nel pc dello sperimentatore principale

Principi Fondamentali – Base Giuridica

I principi fondamentali in materia di protezione dei dati sono “liceità, correttezza e trasparenza” nonché di minimizzazione” del dato; i dati personali sono “trattati in modo lecito, corretto e trasparente nei confronti dell’interessato” e sono “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati” (art. 5, § 1, lett. a) e c) del Regolamento.

I principi secondo i quali i dati dovranno essere trattati sono:

- liceità
- correttezza
- trasparenza
- minimizzazione dei dati.

La base giuridica è l’obbligo legale al quale è soggetto il titolare del trattamento (art. 6, § 1, lett c) del Regolamento), e, con riguardo a categorie particolari di dati (art. 9, § 2, lett. g) del Regolamento) in relazione all’art. 54-bis, o a dati relativi a condanne penali e reati, possono, altresì, essere considerati necessari per l’esecuzione di un compito di interesse pubblico.

Qual è il periodo di conservazione dei dati?

I dati vengono conservati per una durata di sei mesi dal completamento dello studio; al termine dei sei mesi i dati vengono distrutti.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Ai sensi dell’**art. 110 d.lgs. 196/2003 (Codice Privacy)** “ 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. In tali

casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato"

Ove applicabile: come si ottiene il consenso degli interessati?

Vedi sopra

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

Non ci sono Responsabili esterni.

Il promotore principale provvederà a trasmettere il file ai propri collaboratori partecipanti allo studio tramite posta elettronica in modalità criptata

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

I dati non sono trasferiti fuori UE.

Rischi

Tipologie delle fonti di rischio

Potenziali:

- Attacco hacker

Valutazione dell'impatto sui dati personali

Valutazione della perdita di riservatezza

Nell'ambito dell'operazione di trattamento Raccolta retrospettiva, l'impatto derivante dalla perdita di riservatezza è considerato **BASSO** in quanto l'indesiderato attacco hacker è solo potenziale e nel caso in cui il fatto si realizzasse questo non comporterebbe un impatto significativo sulla reputazione.

Valutazione della perdita di integrità

Nell'ambito dell'operazione di trattamento Raccolta retrospettiva, l'impatto derivante dalla perdita di integrità è considerato **BASSO** in quanto il sistema in uso racchiude in sé una serie di protezioni sufficienti a livello informatico.

Valutazione della perdita di disponibilità

Nell'ambito dell'operazione di trattamento Raccolta retrospettiva, l'impatto derivante dalla perdita di disponibilità è considerato **BASSO** in quanto viene utilizzato un pc aziendale adeguatamente protetto e accessibile solo con credenziali personali, oltre ad essere posizionato in stanza chiusa a chiave.

Valutazione di impatto complessiva

Riservatezza	Integrità	Disponibilità
BASSO	BASSO	BASSO
Totale valutazione d'impatto		BASSO

Valutazione della probabilità

Si applica la seguente scala dei valori al questionario di valutazione

Punteggio livello di rischio				
AREA		GLOBALE		
0 - 1	Basso	1	Basso	E' improbabile che la minaccia si realizzi
2 - 3	Medio	2	Medio	C'è una ragionevole possibilità che la minaccia si realizzi
4 - 5	Alto	3	Alto	La minaccia potrebbe materializzarsi

(Risposte: 1 SI; 0 NO; 0,5 Non so)

A	Area: RISORSE DI RETE E TECNICHE			
1	Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?	SI	1	Trasmissione dei dati tramite posta elettronica.
2	È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?	NO	0	
3	Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO	0	
4	Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO	0	

5	Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?	NO	0	
A	Punteggio totale area A		1	BASSO
B	Area: PROCESSI /PROCEDURE RELATIVE ALL'OPERAZIONE DI TRATTAMENTO DEI DATI			
6	I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO	0	incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema.
7	L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO	0	
8	I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO	0	
9	I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	SI	1	trasmissione di informazioni attraverso canali di rete
10	Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO	0	
B	Punteggio totale area B		1	BASSO
C	Area: Parti/Persone coinvolte nel trattamento dei dati personali			
11	Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO	0	
12	Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO	0	

13	Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO	0	
14	Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO	0	
15	Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO	0	
C	Punteggio totale area C		0	BASSO
D	Area: Settore di attività e scala del trattamento			
16	Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO	0	
17	La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	NO	0	
18	Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO	0	
19	Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO	0	
20	Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO	0	
D	Punteggio totale area D		0	BASSO

Valutazioni probabilità di area

- **Risorse di rete e tecniche:** la probabilità di occorrenza di una minaccia è considerata di valore **BASSO (1)**, poiché il sistema è connesso a Internet ed è pur sempre probabile per quanto remota la possibilità di un attacco hacker.
- **Processi / Procedure relative al trattamento dei dati personali:** la probabilità di occorrenza di una minaccia è di valore **BASSO (1)**, in quanto la trasmissione di informazioni attraverso canali di rete sottopone comunque il sistema ad una vulnerabilità.
- **Parti / Persone coinvolte nel trattamento dei dati personali:** la probabilità di occorrenza di una minaccia è di valore **BASSO (0)**. Il trattamento viene eseguito da un numero predefinito di dipendenti di Azienda Asl Toscana NordOvest. Il backup dei dati è assicurato centralmente e regole per la dismissione sicura degli apparati di registrazione di massa sono contenute nel regolamento di utilizzo degli strumenti informatici e istruzioni già operative.
- **Settore di operatività e scala/dimensione del trattamento** la probabilità di occorrenza di una minaccia è di valore **BASSO (0)** in quanto il settore di operatività potrebbe essere considerato soggetto ad attacchi informatici ma il sistema appare idoneo a limitare gli eventuali danni conseguenti.

Valutazioni probabilità globale

AREA DI VALUTAZIONE	PROBABILITA'	
	LIVELLO	ASSOCIATO
Risorse di rete e tecniche	BASSO	1
Processi / Procedure relative al trattamento dei dati personali	BASSO	1
Parti / Persone coinvolte nel trattamento dei dati personali	BASSO	0
Settore di attività e scala di trattamento	BASSO	0
Probabilità complessiva di occorrenza di una minaccia		2

Livello di Rischio Probabilità Globale		
4 - 5	Basso	Verde
6 - 7	Medio	Giallo
8 - 9	Alto	Rosso

Applicando la tabella di riferimento di cui sopra la Probabilità Globale si valuta **BASSA**. Si considera la valutazione adeguata per l'ambito di trattamento in esame.

Calcolo del Rischio Iniziale

RISCHIO RILEVATO = Probabilità (Media) x Impatto (Medio) = Rischio MEDIO (M)

probabilità	Alta			
	Media			
	Bassa	X		
		Impatto		

Misure esistenti o pianificate

Rivalutazione del Rischio

Rivalutazione impatto

Rischio	Impatto
Riservatezza - Accesso Illegittimo ai Dati	
Integrità - Modifiche Indesiderate ai dati	
Disponibilità – Perdita di dati	

Rivalutazione probabilità

Area	Probabilità
Risorse di rete e tecniche	
Processi / Procedure relative al trattamento dei dati personali	
Parti / Persone coinvolte nel trattamento dei dati personali	
Settore di operatività e scala/dimensione del trattamento	

Rischio residuo stimato

Probabilità	Alta			
	Media			
	Bassa			
		Basso	Medio	Alto/Molto Alto
		Impatto		

Piano d'azione

Principi fondamentali

Misure esistenti o pianificate

Rischi accettati

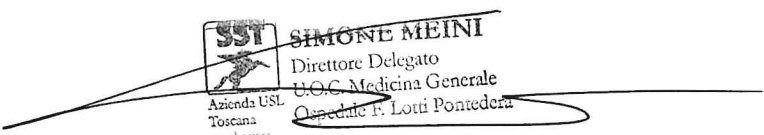
Opinione delle persone interessate o dei loro rappresentanti

Approvazione

Convalida formale da parte

Validato 30/10/2024

Dr. Simone Meini



SST
Azienda USL
Toscana
nord ovest

SIMONE MEINI
Direttore Delegato
U.O.C. Medicina Generale
Ospedale F. Lotti Pontedera