

**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**

Azienda Unità Sanitaria Locale di Reggio Emilia

IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



Presidio Ospedaliero Provinciale Santa Maria Nuova

Arcispedale Santa Maria Nuova di Reggio Emilia

Dipartimento Oncologico e Tecnologie Avanzate

Ematologia

Il Direttore Dr. Francesco Merli

VALUTAZIONE D'IMPATTO PER PROGETTI DI RICERCA IN AMBITO SANITARIO

SU DATI RETROSPETTIVI

(ART. 110 D. LGS. 196/2003, Provvedimento Garante n. 146/2009)

La valutazione di impatto (DPIA) 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.

A CURA DEL RICERCATORE

Titolo dello studio: Studio retrospettivo sull'efficacia e sicurezza di trattamenti comprendenti l'anticorpo monoclonale anti-CD38 daratumumab in pazienti affetti da Mieloma Multiplo ed eventuali associazioni con fattori clinici, terapeutici e genetici

Codice di Protocollo: (REMM-Dara)

Titolare/i del trattamento: Azienda U.S.L. – IRCCS di Reggio Emilia , *SC Ematologia*

Principal Investigator: Emiliano Barbieri

S.C./S.S.D./Unità SC Ematologia, ASMN IRCCS Viale risorgimento80, Reggio Emilia

Data compilazione 24/04/2024

Ematologia

Viale Risorgimento, 80 - 42123 Reggio Emilia

T. +39.0522.296.618 - 296.623 - 296.661 - Fax +39.0522.296.694

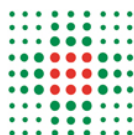
merli.francesco@ausl.re.it

Sede Legale: Via Amendola, 2 - 42122 Reggio Emilia

T. +39.0522.335.111 – Fax +39.0522.335.205

C.F. e Partita IVA 01598570354

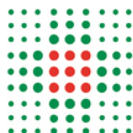
www.ausl.re.it

**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA****Azienda Unità Sanitaria Locale di Reggio Emilia**

IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

**Presidio Ospedaliero Provinciale Santa Maria Nuova
Arcispedale Santa Maria Nuova di Reggio Emilia
Dipartimento Oncologico e Tecnologie Avanzate
Ematologia****Il Direttore Dr. Francesco Merli**

TRATTAMENTO DEI DATI	
Descrizione del trattamento (compilare i campi successivi o allegare il modulo di fattibilità dello studio)	
Sinossi dello Studio	Studio non interventistico, osservazionale, retrospettivo rivolto a pazienti che rispettano i seguenti criteri d'inclusione: Saranno considerati arruolabili tutti i pazienti con diagnosi di MM che hanno ricevuto una terapia a base dell'anticorpo monoclonale anti-CD38 daratumumab presso l'Unità Operativa Complessiva di Ematologia dell'AUSL-IRCCS di Reggio Emilia dal 1 Maggio 2018 al 31 Dicembre 2023.
Tipologia di dati raccolti	
Modalità di raccolta (fonte dei dati) (barrare anche più caselle)	☒ da cartelle cliniche/documentazione sanitaria ☒ da archivi di dati clinici (esempio Dossier Sanitario - DWH) ☒ da archivi di test diagnostici ☒ da dati di laboratorio ☒ da database amministrativi ☐ altro (specificare) _____
Trattamento dei dati (indicare il supporto utilizzato per la rilevazione e conservazione dei dati)	☒ In formato cartaceo ☒ In formato digitale ☐ altro (specificare) _____
Categorie di persone interessate	☒ pazienti ☐ persone sane ☐ operatori sanitari ☐ altro (specificare) _____



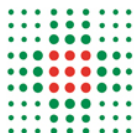
**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



Presidio Ospedaliero Provinciale Santa Maria Nuova
Arcispedale Santa Maria Nuova di Reggio Emilia
Dipartimento Oncologico e Tecnologie Avanzate
Ematologia

Il Direttore Dr. Francesco Merli

Categorie di dati trattati	X dati sulla salute fisica o psichica X dati genetici ☐ informazioni sulla vita sessuale ☐ informazioni sull'orientamento sessuale X informazioni sugli stili di vita e/o le condizioni socioeconomiche ☐ informazioni su istruzione e formazione professionale X anamnesi lavorativa ☐ informazioni su religione o altre credenze ☐ <i>altro (specificare)</i> _____
I dati personali (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati/condivisi con altri?	X no Se sì, selezionare uno o più ambiti di comunicazione: Promotore CRO
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	



**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

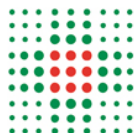


Presidio Ospedaliero Provinciale Santa Maria Nuova
Arcispedale Santa Maria Nuova di Reggio Emilia
Dipartimento Oncologico e Tecnologie Avanzate
Ematologia

Il Direttore Dr. Francesco Merli

Verranno conservati i dati identificativi dei partecipanti?	NO
Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca	Per non identificare direttamente l'interessato sono adottate le seguenti misure: ☐ Adozione di tecniche crittografiche ☒ 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 _____ _____

PRINCIPI, FINALITA' E BASI GIURIDICHE	
Necessità e proporzionalità	
Sono trattati solo i dati necessari e pertinenti al perseguimento delle finalità della ricerca (Minimizzazione)?	☒ 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?	☒ Sì ☐ No Se no, specificare i motivi e le azioni previste _____ _____ _____



**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**

Azienda Unità Sanitaria Locale di Reggio Emilia

IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



Presidio Ospedaliero Provinciale Santa Maria Nuova

Arcispedale Santa Maria Nuova di Reggio Emilia

Dipartimento Oncologico e Tecnologie Avanzate

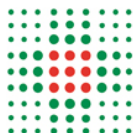
Ematologia

Il Direttore Dr. Francesco Merli

Limitazione della conservazione	
Per quanto tempo verranno conservati i dati raccolti?	Indicare il numero di mesi/anni : come da procedure aziendali per i dati contenuti in cartella clinica informatizzata. 7 anni dal termine dello studio per i documenti studio specifici. Decorso tale termine i dati verranno: Distrutti
Basi giuridiche	
Quali sono le basi giuridiche del trattamento?	art. 110, co. 1, secondo periodo Codice Privacy ¹

MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO	
Informativa e consenso	
SOLO SE LA BASE GIURIDICA È L'ART. 110, CO. 1, SECONDO PERIODO <i>Indicare i motivi per i quali non è possibile fornire l'informativa ai partecipanti allo Studio (soggetti interessati) e acquisirne il consenso</i>	☐ motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione x sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati in ragione: o 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 X sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati e il programma di ricerca comporta l'utilizzo di campioni

¹ 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.



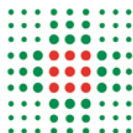
**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



Presidio Ospedaliero Provinciale Santa Maria Nuova
Arcispedale Santa Maria Nuova di Reggio Emilia
Dipartimento Oncologico e Tecnologie Avanzate
Ematologia

Il Direttore Dr. Francesco Merli

	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 DPR	
<i>E' stata predisposta una procedura ad hoc da parte dell'Ente?</i>	☒ Sì ☐ No



**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

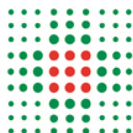


Presidio Ospedaliero Provinciale Santa Maria Nuova
Arcispedale Santa Maria Nuova di Reggio Emilia
Dipartimento Oncologico e Tecnologie Avanzate
Ematologia

Il Direttore Dr. Francesco Merli

A CURA DELL'AZIENDA U.S.L – IRCCS DI REGGIO EMILIA

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO		
MISURA	Esistenti	Note
Organigramma interno	X	
Nomine responsabili esterni	X	
Nomina DPO	X	
Informativa	X	
Istruzioni persone autorizzate trattamento	X	
Formazione	X	
Registri	X	
Procedure	X	
Politiche di tutela della privacy	X	
Distruzione/smaltimento sicuro cartaceo	X	
Inventario degli asset	X	
Misure anti – intrusive (cartelli di divieto di accesso ai locali, strumenti per la rilevazione degli accessi, guardiana, portineria, serrature armadi, schedari, ecc.)	X	
Politiche di sicurezza informatica	X	
Controllo accessi (log)	X	
Antivirus / firewall	X	
Politiche di clear screen	X	
Back – up dei dati	X	
Politiche di trasmissione dei dati nel caso si utilizzi un sito web esterno:	Allegare alla DPIA il Modulo relativo all'Archiviazione e Rilevazione Dati Per Attività di Ricerca su Sistemi Informativi	
Connessione sicura		
Accesso protetto da utenza personale		
Crittografia		
Anonimizzazione		
Pseudonimizzazione		
Sicurezza dei documenti cartacei	X	
Gestione postazioni	X	
Autenticazione	X	
Policy di gestione data breach	X	
Altro:		



**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**

Azienda Unità Sanitaria Locale di Reggio Emilia

IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



Presidio Ospedaliero Provinciale Santa Maria Nuova

Arcispedale Santa Maria Nuova di Reggio Emilia

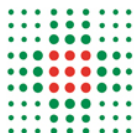
Dipartimento Oncologico e Tecnologie Avanzate

Ematologia

Il Direttore Dr. Francesco Merli

APPENDICE

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; accesso non autorizzato all'archivio delle cartelle cliniche dei pazienti arruolati nello studio; virus Quali sono le fonti di rischio? Fonti umane interne (lasciare incustodita la postazione di lavoro, lasciare incustodite sulla scrivania le cartelle cliniche dei pazienti arruolati nello studio, 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; Anonimizzazione; Pseudonimizzazione Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? Media 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 cura del paziente



**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**

Azienda Unità Sanitaria Locale di Reggio Emilia

IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



Presidio Ospedaliero Provinciale Santa Maria Nuova

Arcispedale Santa Maria Nuova di Reggio Emilia

Dipartimento Oncologico e Tecnologie Avanzate

Ematologia

Il Direttore Dr. Francesco Merli

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; accesso non autorizzato all'archivio delle cartelle cliniche dei pazienti arruolati nello studio; virus

Quali sono le fonti di rischio?

Fonti umane interne (lasciare incustodita la postazione di lavoro, lasciare incustodite sulla scrivania le cartelle cliniche dei pazienti arruolati nello studio, 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

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

Media: nonostante le misure adottate a protezione delle postazioni di lavoro, lo strumento utilizzato per la allocazione dei dati (excel) non è da ritenere del tutto sicuro rispetto alla probabilità di accadimento

PERDITA DI DATI

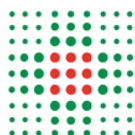
Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Una perdita dei dati potrebbe essere sia informatica che cartacea; in entrambi i casi potrebbe causare l'alterazione dei risultati dello Studio o la impossibilità di proseguire lo Studio

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; accesso non autorizzato ai locali archivio causando la sottrazione del materiale cartaceo, se il formato cartaceo è l'unico sistema di conservazione del dato e non esiste alcun backup). Incidente tecnico al datacenter (incendio, inondazione, fulmini...)



**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**

Azienda Unità Sanitaria Locale di Reggio Emilia

IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



Presidio Ospedaliero Provinciale Santa Maria Nuova

Arcispedale Santa Maria Nuova di Reggio Emilia

Dipartimento Oncologico e Tecnologie Avanzate

Ematologia

Il Direttore Dr. Francesco Merli

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; lasciare incustodite sulla scrivania le cartelle cliniche dei pazienti arruolati nello Studio; 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: l'impatto sugli interessati potrebbe essere elevato, tuttavia le misure previste per evitare la perdita dei dati rende 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 e degli archivi cartacei rendono quasi nulla la probabilità di accadimento

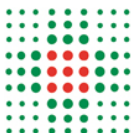
A CURA DEL DPO

VALUTAZIONE DEL RISCHIO

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

MATRICE DI VALUTAZIONE DEL RISCHIO

		IMPATTO^{§§}				
PROBABILITÀ	MOLTO ALTO[§]	5	10	15	20	25
	ALTO	4	8	12	16	20
	MEDIO	3	6	9	12	15



Il Direttore Dr. Francesco Merli

	BASSO	2	4	6	8	10
	MOLTO BASSO	1	2	3	4	5
		MOLTO BASSO	BASSO	MEDIO	ALTO	MOLTO ALTO

99 **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

<u>MINACCIA</u>	<u>VALORE DEL RISCHIO</u> <u>(P*I)</u>	<u>LIVELLO DI RISCHIO</u>	<u>VALUTAZIONE</u> (SOMMA COLONNA LIVELLO RISCHIO)
ACCESSO ILLEGITTIMO	3*1	3	10
MODIFICHE INDESIDERATE DEI DATI	2*3	6	
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