Valutazione d’impatto sulla protezione dei dati

Valutazione d’impatto - 034.010 - Progetto PNRR-MCNT1-2023-12378269 - PI ROSSINI

28/04/2026

Indice

1. Introduzione.....
2. Informazioni essenziali.....
3. Stima del rischio e pre-assessment.....
4. Informazioni sul trattamento.....
5. Valutazione della proporzionalità in relazione alla finalità.....
6. Diritti e principi fondamentali.....
7. Valutazione del rischio.....
    7.1 Misure di sicurezza.....
    7.2 Valutazione del rischio.....
8. Coinvolgimento delle parti interessate.....
9. Note.....

1. Introduzione

Il presente documento “Valutazione d’impatto - 034.010 - Progetto PNRR-MCNT1-2023-12378269 - PI ROSSINI” ha lo scopo di valutare l’impatto sulla protezione dei dati dell’attività di trattamento “Progetto PNRR-MCNT1-2023-12378269 - PI ROSSINI”, l’impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati.

2. Informazioni essenziali

Data di creazione dell’analisi	23/10/2025
Data generazione documento	28/04/2026
Data del prossimo controllo	12/12/2026
Stato	In lavorazione
Reporter	Ilaria Del Giglio

3. Stima del rischio e pre-assessment

Pre-Assessment

Tipologia del trattamento	Risposta
Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l’affidabilità o il comportamento, l’ubicazione o gli spostamenti dell’interessato.	No
Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi).	No

Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.	No
Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 Regolamento UE 2016/679 interconnessi con altri dati personali raccolti per finalità diverse.	Sì
Trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).	Sì
Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).	No
Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).	Sì
Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 (criteri WP 29).	No
Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.	No
Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	No

Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	No

Stima del rischio

Criteri utilizzati per la stima del rischio	Risposta
Il trattamento comporta la valutazione o assegnazione di un punteggio inclusiva di profilazione e previsione	No
Il trattamento prevede un processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente	No
Il trattamento consiste in un'attività di monitoraggio sistematico	No
Il trattamento coinvolge dati sensibili o dati aventi carattere altamente personale	Sì
Il trattamento di dati avviene su larga scala	Sì
Il trattamento comporta la creazione di corrispondenze o combinazione di insiemi di dati	No
Il trattamento coinvolge categorie di interessati vulnerabili	Sì
Il trattamento coinvolge l'uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	No
Il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	No
Elevato	

4. Informazioni sul trattamento

Codice identificativo	Nome	Data di creazione	Data dell'ultima modifica
034.010	Progetto PNRR-MCNT1-2023-12378269 - PI ROSSINI	23/10/2025	13/04/2026
Descrizione			
Studio osservazionale prospettico e retrospettivo multicentrico non profit, finanziato dal Ministero della Salute (PNRR M6/C2_CALL 2023), finalizzato a determinare l'associazione tra esposizione acuta all'inquinamento atmosferico ambientale (particolato PM10) e il rischio di riacutizzazioni dell'artrite reumatoide (AR) in pazienti adulti. Lo studio include: (1) analisi caso-crossover per valutare la correlazione tra inquinanti atmosferici e ricadute della malattia; (2) valutazione di biomarcatori sierici associati a infiammazione e danno tissutale; (3) studio proteomico per identificare proteine correlate all'esposizione ambientale. I dati clinici e anamnestici vengono raccolti in forma retrospettiva e prospettica, pseudonimizzati mediante tecnica del "contatore" e gestiti			

tramite piattaforma REDCap. Lo studio prevede anche prelievi ematici per analisi biochimiche e proteomiche. La ricerca coinvolge tre centri italiani (Verona-Promotore, Foggia, Messina).	
Finalità del trattamento	
Ricerca scientifica in campo medico, biomedico ed epidemiologico per determinare l'associazione tra esposizione all'inquinamento atmosferico (particolato PM10) e gravità della malattia e rischio di riacutizzazione nell'Artrite Reumatoide (AR), Obiettivi specifici:, • Determinare l'associazione tra concentrazione di inquinanti atmosferici (PM10) e ricadute dell'AR (studio caso-crossover), • Valutare biomarcatori sierici associati a infiammazione e danno tissutale, • Studio proteomico per identificare proteine associate all'esposizione all'inquinamento	
Basi giuridiche	
Articolo 6 a) – l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità	
Articolo 9 a) – l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche	
Riferimenti normativi	
Per pazienti viventi e contattabili:, Articolo 6 a) GDPR - l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità, Articolo 9 a) GDPR - l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, Per pazienti deceduti:, Articolo 110 del d.lgs. 196/2003 come modificato dal D.L. n. 19/2024, Misure di garanzia individuate dal Garante con provvedimento n. 298 del 9/5/2024, Riferimenti Normativi, Art. 89, Regolamento UE 2016/679, Art. 110, d.lgs. 196/2003 come modificato, Provvedimento del Garante n. 298 del 9/5/2024 recante le misure di garanzia	
Origine dei dati	
Raccolti presso l'interessato	
Dati già raccolti (Raccolti presso l'interessato (dati prospettici) Già presenti nei sistemi del Titolare (dati retrospettivi) Modalità di raccolta: • Raccolta retrospettiva da cartelle cliniche e database aziendali esistenti • Raccolta prospettica attraverso visite cliniche programmate, questionari, prelievi ematici)	
Modalità del trattamento	
Cartaceo	Informatizzato
Categorie di dati	
Categorie particolari di dati personali	
Particolari	Dati relativi alla salute
	Campioni biologici
Dati personali comuni	

Personali	Dati anagrafici
	Dati di identificazione (codice paziente)
	Comune di residenza (codice ISTAT)
Categorie di interessati	Pazienti ; Persone decedute ; Soggetti arruolati negli studi clinici ; Sperimentatori
Titolare	Azienda Ospedaliera Universitaria Integrata Verona
Contitolari del trattamento	Azienda Ospedaliera Universitaria Gaetano Martino Messina ; Azienda Ospedaliero-Universitaria "Policlinico Riuniti" Foggia
Responsabili del trattamento	Centro Piattaforme Tecnologiche (CPT) - Centro di Servizio
Responsabile della protezione dei dati	Compliance Officer e Data Protection di Polito Dott.ssa Filomena ; Filomena Polito
Diffusione dei dati	Non viene effettuata la diffusione dei dati.

Trasferimenti e comunicazioni dei dati	
Il trattamento prevede il trasferimento o la comunicazione di dati	
Comunicazioni	
Destinatari	**Note**
Centro partecipante autonomo titolare del trattamento per condivisione dati di ricerca scientifica	Comunicazione di dati personali tra il Promotore (AOUI Verona) e il/i Centro/i partecipante/i, tutti qualificati come autonomi titolari del trattamento per le rispettive competenze per la conduzione dello studio.
Centro promotore - Responsabile del trattamento ; Centro Piattaforme Tecnologiche (CPT) - Centro di Servizio	Il trasferimento dei campioni biologici e dei dati associati dal Promotore (UOC Reumatologia - AOUI Verona) al CPT

Periodo di conservazione dei dati personali	10 anni
Descrizione del periodo di conservazione dei dati	
Durata studio: 24 mesi di follow-up Campioni biologici: saranno scartati al termine dello studio Dati personali: Conservati per 10 anni, poi anonimizzati	

Applicativi	File Excel per la ricerca - Misura di sicurezza specifica per la gestione protetta di file Excel utilizzati temporaneamente nella raccolta e organizzazione di dati di ricerca prima del loro trasferimento su piattaforme dedicate. Include crittografia dei file, protezione tramite password, firma digitale con hash per garantire l'integrità, accesso limitato al personale autorizzato e archiviazione su server di rete sicuri con autenticazione controllata. Ambito di applicazione: File Excel contenenti dati sensibili utilizzati in attività di ricerca clinica e scientifica per raccolta, organizzazione e trasferimento dati verso sistemi definitivi di conservazione. Finalità: Garantire la sicurezza, integrità e riservatezza dei dati personali e sensibili durante la fase di raccolta temporanea, assicurando conformità alle normative sulla protezione dei dati e minimizzando i rischi di accesso non autorizzato o alterazione delle informazioni. ; RedCap - REDCap (Research Electronic Data Capture) è una piattaforma web progettata per supportare l'acquisizione e l'archiviazione di dati per studi clinici.

Descrizione sistematica delle componenti del trattamento

Descrizione delle diverse componenti tecnologiche, fisiche ed organizzative che partecipano dell'attività di trattamento valutata.

Componenti organizzative

Componente	Descrizione
Soggetti Interni	**Descrizione sintetica (es. soggetti facenti parte o meno del personale tecnico informatico, descrizione delle attività svolte in relazione ai trattamenti in esame, formazione ricevuta, procedure che ne disciplinano le mansioni, relazioni con altre componenti**
	Soggetti interni Sperimentatori: medici e sanitari dipendenti del Titolare o medici/sanitari universitari di Univr inseriti in assistenza
Soggetti Esterni	**Descrizione sintetica (es. caratteristiche del servizio erogato o del titolo che giustifica il coinvolgimento di tale soggetto, presenza di un accordo sul trattamento di dati, relazioni con altre componenti)**
	come da descrizione del trattamento

Componenti tecnologiche

Componente	Descrizione

Applicazioni	**Descrizione sintetica (es. principali caratteristiche, funzionalità, modalità di autenticazione, relazioni con altre componenti)**
	REDCap I dati risiedono sulla piattaforma REDCap di proprietà di AOUI (https://redcap.aovr.veneto.it) e verranno raccolti utilizzando una eCRF (electronic Case Report Form) creata appositamente per lo Studio. Il software REDCap (Research Electronic Data Capture) è una piattaforma web progettata per supportare l'acquisizione e l'archiviazione di dati per studi di ricerca; integra un sistema di gestione privilegi utente per controllare l'esportazione, la visualizzazione e la modifica dei dati e fornisce percorsi di verifica per monitorare la manipolazione dei dati e le procedure di esportazione. Seguendo il metodo del contatore come metodo di pseudonimizzazione come da Linee guida ENISA, novembre 2019, la piattaforma genera un codice numerico univoco associato ad ogni soggetto coinvolto nello Studio, che consente ai ricercatori di mantenere localmente l'associazione con i rispettivi dati anagrafici. La possibilità di risalire all'origine dei dati è giustificata dalla necessità di effettuare studi di follow up per i pazienti in cura presso le Unità Operative coinvolte, oppure in caso di risultati scientifici che possano avere un impatto rilevabile per il soggetto stesso, sulla base di decisioni espresse nel consenso informato alla partecipazione allo Studio. REDCap è installato su server di AOUI e vengono effettuati backup giornalieri; la connessione con la piattaforma è cifrata con certificato digitale SSL e l'accesso alla banca dati è consentito solo al personale addetto allo Studio ed avviene mediante account REDCap con autenticazione a due fattori (2FA). L'accesso avviene con nome utente e una password (primo fattore) di almeno quindici caratteri, tra cui almeno un numero, una lettera maiuscola, una lettera minuscola e un carattere speciale, che viene cambiata ogni mese; il secondo fattore è un codice numerico a scadenza temporale che viene inviato sulla mail collegata all'account. Excel Il file Excel con cui vengono temporaneamente raccolti i dati da inserire in REDCap è criptato e protetto tramite password. L'accesso è limitato al solo personale autorizzato.Il file Excel è conservato sulle cartelle di rete della UOC presenti sul server del trattamento. L'accesso avviene mediante autenticazione dell'utente, abilitato ad accedere a quelle determinate cartelle di rete. L'utente accede mediante ID e password che viene cambiata periodicamente ogni 3 mesi. Una volta compiute le elaborazioni, il file Excel viene cancellato in modo che l'unico software di conservazione dei dati sia REDCap.
Infrastrutture IT	**Descrizione sintetica (es. principali caratteristiche tecniche e relazioni con altre componenti)**
	come da descrizione del trattamento
Rete	**Descrizione sintetica (es. tipologia di rete, tecnologie utilizzate, relazioni con altre componenti)**

	rete Aziendale rete internet mediante connessione sicura

Componenti fisiche

Componente	Descrizione
Risorse ed asset materiali	**Descrizione (es. principali caratteristiche, tipologia di asset non latamente inteso come informatico, relazioni con altre componenti)**
	come da descrizione del trattamento
Sedi fisiche	**Descrizione (es. ubicazione delle sedi anche distaccate o periferiche, principale utilizzo, relazioni con altre componenti)**
	come da descrizione del trattamento

5. Valutazione della proporzionalità in relazione alla finalità

Tenuto conto che l'attività di trattamento sottoposta a valutazione comporta il trattamento delle categorie di dati personali sopra menzionati, in relazione alle categorie di interessati precedentemente citati, il titolare ritiene che dette categorie di dati siano necessarie e proporzionali al perseguimento della finalità:

Ricerca scientifica in campo medico, biomedico ed epidemiologico per determinare l'associazione tra esposizione all'inquinamento atmosferico (particolato PM10) e gravità della malattia e rischio di riacutizzazione nell'Artrite Reumatoide (AR)
Obiettivi specifici:
• Determinare l'associazione tra concentrazione di inquinanti atmosferici (PM10) e ricadute dell'AR (studio caso-crossover)
• Valutare biomarcatori sierici associati a infiammazione e danno tissutale
• Studio proteomico per identificare proteine associate all'esposizione all'inquinamento

6. Diritti e principi fondamentali

Diritti

Accesso	Le informazioni previste dall'art. 13 e art. 14 par. 5 lett. b) GDPR sono rese disponibili in modo trasparente e facilmente accessibile agli interessati. Esse sono riportate nell'informativa che viene consegnata agli interessati prima dell'arruolamento. La medesima è stata pubblicata sul sito intenet aziendale per consentire la diffusione della medesima nel caso di pazienti irreperibili. Le richieste di accesso sono gestite seguendo una procedura aziendale dedicata, che garantisce l'organizzazione e la corretta gestione di tali richieste. Per assicurare che i dati vengano resi disponibili soltanto all'interessato, prima di procedere con l'evasione di una richiesta, ne viene attentamente verificata l'identità.

Rettifica	I soggetti interessati possono esercitare in ogni momento il diritto di rettifica dei dati personali inesatti che li riguardano. Vale al riguardo quanto previsto dall'art. 110, comma 2, del d.lgs. 196/2003, per cui “in caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 16 del regolamento nei riguardi dei trattamenti di cui al comma 1, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca”. Le informazioni previste dall'art. 13 e art. 14 par. 5 lett. b) GDPR sono rese disponibili in modo trasparente e facilmente accessibile agli interessati. Esse sono riportate nell'informativa che viene consegnata agli interessati prima dell'arruolamento. La medesima è stata pubblicata sul sito intenet aziendale per consentire la diffusione della medesima nel caso di pazienti irreperibili.
Cancellazione	I soggetti interessati hanno il diritto di ottenere dal Titolare la cancellazione dei dati personali che li riguardano, qualora sussista uno dei motivi indicati nell'art. 17, par. 1, del RGPD. Resta fermo che, in caso di revoca del consenso da parte dell’interessato, non saranno raccolti ulteriori dati che lo riguardano, ma quelli eventualmente già raccolti potranno essere utilizzati per determinare, senza alterarli, i risultati della ricerca. Le informazioni previste dall'art. 13 e art. 14 par. 5 lett. b) GDPR sono rese disponibili in modo trasparente e facilmente accessibile agli interessati. Esse sono riportate nell'informativa che viene consegnata agli interessati prima dell'arruolamento. La medesima è stata pubblicata sul sito intenet aziendale per consentire la diffusione della medesima nel caso di pazienti irreperibili.
Portabilità	Le informazioni previste dall'art. 13 e art. 14 par. 5 lett. b) GDPR sono rese disponibili in modo trasparente e facilmente accessibile agli interessati. Esse sono riportate nell'informativa che viene consegnata agli interessati prima dell'arruolamento. La medesima è stata pubblicata sul sito intenet aziendale per consentire la diffusione della medesima nel caso di pazienti irreperibili.
Opposizione	Gli interessati possono esercitare il diritto di opposizione al trattamento ricorrendo le condizioni di cui all'art. 21, par. 1, del GDPR; inoltre, ai sensi dell’art. 21, par. 6, del GDPR l’interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento sia necessario per l’esecuzione di un compito di interesse pubblico e sempre previa richiesta scritta. Le informazioni previste dall'art. 13 e art. 14 par. 5 lett. b) GDPR sono rese disponibili in modo trasparente e facilmente accessibile agli interessati. Esse sono riportate nell'informativa che viene consegnata agli interessati prima dell'arruolamento. La medesima è stata pubblicata sul sito intenet aziendale per consentire la diffusione della medesima nel caso di pazienti irreperibili.

Limitazione di trattamento	I soggetti interessati hanno il diritto di ottenere dal Titolare la limitazione del trattamento quando ricorra una delle ipotesi previste dall'art. 18, par. 1, del GDPR. Le informazioni previste dall'art. 13 e art. 14 par. 5 lett. b) GDPR sono rese disponibili in modo trasparente e facilmente accessibile agli interessati. Esse sono riportate nell'informativa che viene consegnata agli interessati prima dell'arruolamento. La medesima è stata pubblicata sul sito internet aziendale per consentire la diffusione della medesima nel caso di pazienti irreperibili.
Revoca del consenso	Le informazioni previste dall'art. 13 e art. 14 par. 5 lett. b) GDPR sono rese disponibili in modo trasparente e facilmente accessibile agli interessati. Esse sono riportate nell'informativa che viene consegnata agli interessati prima dell'arruolamento. La medesima è stata pubblicata sul sito intenet aziendale per consentire la diffusione della medesima nel caso di pazienti irreperibili.
Diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato	Non viene compiuto alcun trattamento che comporti una decisione basata unicamente su un trattamento automatizzato.

Principi

I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato	I dati vengono raccolti per essere utilizzati per scopi scientifici riferiti allo Studio. Tutte le informazioni raccolte sono adeguate e pertinenti, in quanto volte unicamente alla definizione dei fattori di rischio, del quadro clinico, dei fattori prognostici e delle possibilità terapeutiche attuali o future. Tutti i dati raccolti saranno trattati da personale competente nelle patologie interessate previamente autorizzato al trattamento ex art. 29, GDPR, ovvero designato di specifici compiti ex art. 2-quaterdecies, d.lgs. 196/2003, debitamente istruito e che valuterà l'esattezza degli stessi e il rispetto del protocollo dello Studio. Il database sul quale i dati vengono registrati è dotato di sistemi automatici di validazione, in grado di rilevare possibili incongruenze. Prima dell'acquisizione dei dati, lo sperimentatore, o un suo delegato autorizzato, rende a ciascun paziente contattabile idonea informativa e rende informativa pubblica, ai sensi dell'art. 14 par. 5 lett. b), al fine di informare e acquisire i seguenti consensi: (a) a partecipare allo Studio, con modulo separato; (b) al trattamento dei dati personali necessari per lo Studio; (c) alla pubblicazione dei dati personali relativi allo Studio in forma pseudonimizzata, in occasione di convegni scientifici o per pubblicazioni scientifiche; (d) al trasferimento dei dati verso Paesi terzi [se pertinente]; (e) a conoscere i risultati dello Studio, qualora comportino per l'Interessato un beneficio concreto e diretto in termini di terapia, prevenzione o di consapevolezza delle scelte riproduttive, ove necessario unitamente a un'appropriata consulenza genetica [se pertinente per studi con dati genetici]; (f) a conoscere eventuali notizie inattese, qualora queste ultime rappresentino per l'Interessato un beneficio concreto e diretto in termini di terapia o di prevenzione o di consapevolezza delle scelte riproduttive [se pertinente per studi con dati genetici]; (g) a comunicare i risultati dello Studio, qualora comportino un beneficio concreto e diretto in termini di terapia, prevenzione o di consapevolezza delle scelte riproduttive anche per gli appartenenti alla stessa linea genetica dell'Interessato, a questi ultimi, su loro richiesta [se pertinente per studi con dati genetici]. Inoltre, nel trattamento dei dati personali degli interessati in fase di Studio vengono rispettati i principi fondamentali di cui all'art. 5 del GDPR.
I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità	Le finalità del trattamento sono quelle sopra indicate e sono esplicitate nella informativa che viene resa ai pazienti prima dell'inizio del trattamento. Quanto ai trattamenti successivi, i dati saranno utilizzati per contattare i pazienti per valutare la volontà di partecipare a futuri progetti di ricerca debitamente autorizzati dal competente Comitato Etico, previo rilascio dell'informativa e la raccolta del consenso specifico o, nel caso di pazienti deceduti o irreperibili, dal compimento degli adempimenti previsti dall'art. 110 Cod. Privacy e dalle misure di garanzia dettate dal Garante in data 09/05/2024.

I dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati	I dati riguardano soggetti interessati individuati secondo i criteri inclusivi descritti nel protocollo di studio. Tali dati saranno raccolti a partire dall'approvazione dello Studio da parte del CE competente e del compimento di tutti gli adempimenti previsti dall'art. 110 Cod. privacy e dalle misure di garanzia dettate dal Garante. I dati saranno conservati secondo i termini indicati nel protocollo di studio in una forma che non consente di risalire direttamente all'identità degli interessati; trascorso questo periodo, i dati saranno distrutti. La tecnica di pseudonimizzazione impiegata con REDCap è la tecnica del contatore (Linee guida ENISA, novembre 2019) consistente nella sostituzione degli identificativi con un numero progressivo univoco generato automaticamente dal programma.
I dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali	I dati risiedono sulla piattaforma REDCap di proprietà di AOUI (https://redcap.aovr.veneto.it) e verranno raccolti utilizzando una eCRF (electronic Case Report Form) creata appositamente per lo Studio. Il software REDCap (Research Electronic Data Capture) è una piattaforma web progettata per supportare l'acquisizione e l'archiviazione di dati per studi di ricerca; integra un sistema di gestione privilegi utente per controllare l'esportazione, la visualizzazione e la modifica dei dati e fornisce percorsi di verifica per monitorare la manipolazione dei dati e le procedure di esportazione. Seguendo il metodo del contatore come metodo di pseudonimizzazione come da Linee guida ENISA, novembre 2019, la piattaforma genera un codice numerico univoco associato ad ogni soggetto coinvolto nello Studio, che consente ai ricercatori di mantenere localmente l'associazione con i rispettivi dati anagrafici. La possibilità di risalire all'origine dei dati è giustificata dalla necessità di effettuare studi di follow up per i pazienti in cura presso le Unità Operative coinvolte, oppure in caso di risultati scientifici che possano avere un impatto rilevabile per il soggetto stesso, sulla base di decisioni espresse nel consenso informato alla partecipazione allo Studio. REDCap è installato su server di AOUI e vengono effettuati backup giornalieri; la connes_x0002_sione con la piattaforma è cifrata con certificato digitale SSL el'accesso alla banca dati è consentito solo al personale addetto allo Studio e avviene mediante account REDCap con autenticazione a due fattori (2FA). L'accesso avviene con nome utente e una password (primo fattore) di almeno quindici caratteri, tra cui almeno un numero, una lettera maiuscola, una lettera minuscola e un carattere speciale, che viene cam_x0002_biata ogni mese; il secondo fattore è un codice numerico a scadenza temporale che viene inviato sulla mail collegata all'account.

7. Valutazione del rischio

Al fine di calcolare la magnitudo di un rischio e si adotta una formula del tipo

$R_1 = f(M, p)$

IMPATTO (M)

LIEVE	1
MEDIO	2
ALTO	3
ALTISSIMO	4

X

PROBABILITÀ (p)

IMPROBABILE	1
POCO PROBABILE	2
PROBABILE	3
ALTAMENTE PROBABILE	4

=

RISCHIO INIZIALE (R)

BASSO	1 - 2
MEDIO	3 - 4
ALTO	5 - 8
ALTISSIMO	9 - 16

Dove per:

- **R** si intende il livello di rischio non mitigato;
- **M** si intende l'impatto per i diritti e le libertà degli interessati che viene indicato assegnando un valore da uno a quattro secondo la seguente scala:

Lieve	Gli interessati non saranno coinvolti o nella peggiore delle ipotesi potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema.
Medio	Gli interessati potrebbero incontrare degli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà
Grave	Gli interessati potrebbero incontrare conseguenze significative, che dovrebbero essere in grado di far fronte seppur con gravi difficoltà
Gravissimo	Gli interessati potrebbero confrontarsi con conseguenze significative o irreversibili.

- **p** si intende la probabilità di accadimento del rischio che viene indicata assegnando un valore da uno a quattro secondo la seguente scala:

Improbabile	L'avverarsi della minaccia non sembra possibile
Poco Probabile	L'avverarsi della minaccia sembra difficile
Probabile	L'avverarsi della minaccia sembra possibile
Altamente Probabile	L'avverarsi della minaccia sembra probabile

Un controllo o misura di sicurezza può agire sulla probabilità o l'impatto (o su entrambi) di una minaccia secondo la seguente logica:

$$R_2 = R_1 - (M_n)$$

dove per:

- R_2 si intende il rischio finale, ovverosia il rischio a valle dell'inserimento dei controlli o misure di sicurezza;
- R_1 si intende il rischio iniziale come definito più sopra;
- M_n si intende il controllo o la misura di sicurezza.

All'interno del presente passaggio saranno presenti, in ordine

1. l'elenco di misure di sicurezza, suddivise in misure associate in via diretta all'attività di trattamento (misure di sicurezza c.d. "su trattamenti") ed in misure associate ad un asset (misure di sicurezza su "componenti IT", "applicativi" e "luoghi fisici") correlato a propria volta all'attività di trattamento;
2. l'elenco delle minacce comprensivo di: nome assegnato alla minaccia, fonte del rischio (la quale può essere, anche cumulativamente, umana se relativa a soggetti appartenenti all'organizzazione di colui che effettua la valutazione d'impatto, di contesto se relativa a soggetti non appartenenti all'organizzazione del soggetto che effettua la valutazione d'impatto, afferente a strumenti se correlata a malfunzionamenti di strumentazione anche se dipendenti da eventi esterni quali disastri naturali), area di impatto (disponibilità, integrità, riservatezza, anche cumulativamente), valori relativi ad impatto e probabilità (con eventuale motivazione sulle scelte effettuate) e valore specifico del rischio non mitigato;
3. i controlli o misure di sicurezza adottate o valutate nonché la loro incidenza su impatto e probabilità della minaccia.

   https://doc.privacymanager.eu/manuale/valutazione_impatto.html#mitigazione-del-rischio-iniziale-qualitativa
4. Rischio residuo (mitigato).

7.1 Misure di sicurezza

Misure di sicurezza trasversali relative ai trattamenti

Nessuna misura selezionata

Misure di sicurezza trasversali relative agli asset

Nessuna misura selezionata

Misure di sicurezza specifiche relative al trattamento

Categoria	Misura	Stato di adozione e implementazione
Misure di sicurezza ENISA	Chiara definizione e assegnazione dei ruoli e delle responsabilità relativi al trattamento dei dati personali, in conformità con la politica di sicurezza.	Applicata
	Chiara definizione delle modalità di revoca dei diritti e delle responsabilità degli utenti in caso di riorganizzazioni interne o cessazioni e cambio di impiego, con le rispettive procedure di passaggio di consegne.	Applicata
	Esistenza di una politica dettagliata e documentata di controllo degli accessi, con relativa segregazione dei ruoli.	Applicata
	Utilizzo delle macchine distruggidocumenti, o simili, per l'eliminazione della carta e di supporti portatili utilizzati per memorizzare i dati personali.	Applicata
Misure di sicurezza fisiche	Sistemazione della documentazione in contenitori (armadi, schedari, ecc.) muniti di serratura	Applicata
Misure di sicurezza organizzative	Esistenza di procedure di formazione del personale in materia di protezione dati, compresi i profili di sicurezza	Applicata
	Vincoli di riservatezza per il personale relativamente ai dati personali trattati	Applicata
	Divieto di lasciare incustoditi presso fotocopiatrici e stampanti documenti cartacei contenenti dati personali	Applicata
	Divieto di salvataggio in locale di dati personali	Applicata
	Rilascio di adeguate istruzioni in merito al trattamento dei dati personali a tutti i soggetti coinvolti nella procedura	Applicata
	Attribuzione di specifici compiti e funzioni connessi al trattamento dei dati personali a soggetti espressamente designati	Applicata

	Conservazione chiave di decodifica Descrizione: Conservazione in maniera sicura e separata della chiave di decodifica	Applicata
Misure di sicurezza tecniche	Pseudonimizzazione dei dati	Applicata

Misure di sicurezza specifiche relative agli asset correlati con il trattamento

Asset	Categoria	Misura di sicurezza	Stato di adozione e implementazione
Applicativi			
File Excel per la ricerca	Misure di sicurezza tecniche	Assegnazione e gestione dei privilegi di accesso secondo il principio del privilegio minimo (Profilazione)	Applicata
		Esistenza di regole sul corretto utilizzo e gestione della password di accesso, con obbligo di utilizzo di credenziali di elevata robustezza	Applicata
		Assegnazione ad ogni utente di chiavi di cifratura personali	Applicata
		Cifratura della base dati	Applicata
		Creazione almeno settimanalmente di una copia di sicurezza (backup) necessaria al ripristino del sistema.	Applicata
		Garanzia di immutabilità delle copie di sicurezza.	Applicata

		Firma digitale della base dati con hash Descrizione: Al fine di garantire l'esattezza dei dati conservati sui file Excel, in particolare a quelli afferenti ai pazienti arruolati, i fogli Excel verranno firmati digitalmente attraverso un hash. La firma digitale generata sarà detenuta da un soggetto distinto da quello addetto alla raccolta dati e verrà, nel caso, ripetuta ove i dati vengano modificati o esportati su altri file. Tale misura consente di rafforzare le tutele volte a garantire l'esattezza dei dati e ad assicurare, altresì, che eventuali successive alterazioni degli stessi siano rapidamente rilevate e corrette.	Applicata
	Misure di sicurezza organizzative	Accesso alle risorse sulla base di profili di autorizzazione decisi in funzione della qualifica dell'utente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilita dall'Amministrazione	Applicata

	Misure di sicurezza ENISA	Definizione di documentate procedure di backup e ripristino dei dati.	Applicata
	Misure di sicurezza logiche	Accesso a strumenti di lavoro per la produttività individuale tramite credenziali forti di autenticazione	Applicata
RedCap	Misure di sicurezza tecniche	Assegnazione e gestione dei privilegi di accesso secondo il principio del privilegio minimo (Profilazione)	Applicata
		Esistenza di regole sul corretto utilizzo e gestione della password di accesso, con obbligo di utilizzo di credenziali di elevata robustezza	Applicata
		Accesso ai sistemi con autenticazione forte (es. MFA/CNS/smart card/certificato/firma digitale)	Applicata
		Utilizzo di protocolli di rete sicuri per l'uso dell'applicativo, usando protocolli crittografici (SSL/TLS)	Applicata
		Pseudonimizzazione dei dati	Applicata
		Validazione dell'input a livello di applicazione (SQL Injection)	Applicata
		Timeout delle sessioni dopo N minuti di inattività	Applicata

		Cifratura della base dati	Applicata
		Creazione almeno settimanalmente di una copia di sicurezza (backup) necessaria al ripristino del sistema.	Applicata
		Effettuazione di backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Applicata
		Implementazione di un sistema di audit log e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema	Applicata
		Canali di trasmissione protetti Descrizione: Utilizzo di canali di trasmissione protetti, tenendo conto dello stato dell'arte della tecnologia, e garantiscano, previa verifica, l'identità digitale del server che eroga il servizio e della postazione client da cui si effettua l'accesso ai dati, ricorrendo a certificati digitali emessi in conformità alla legge da un'autorità di certificazione	Applicata

	Misure di sicurezza organizzative	Esistenza di una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata
		Esistenza di controlli periodici sulle utenze rilasciate al fine di garantirne la coerenza.	Applicata
	Misure di sicurezza ENISA	Registrazione delle azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / eliminazione / modifica dei diritti di accesso degli utenti.	Applicata
		In un'ottica di privacy by default, i database e application server devono elaborare solo i dati personali che sono effettivamente necessari per l'elaborazione al fine di raggiungere i propri scopi di elaborazione.	Applicata
		Applicazione di tecniche che supportano la privacy a livello di database, come le authorized queries, il privacy preserving data base querying, la searchable encryption, ecc.	Applicata
		Utilizzo di protocolli di rete sicuri per l'accesso a internet, usando protocolli crittografici (SSL/TLS)	Applicata

		Definizione di documentate procedure di backup e ripristino dei dati.	Applicata
Luoghi fisici			
Il Laboratorio Universitario di Ricerca Medica (LURM) è un Centro Interdipartimentale di Ricerca dell'Università di Verona con autonomia gestionale, amministrativa, finanziaria e di spesa.Al LURM afferiscono diversi Dipartimenti Universitari della Scuola di Medicina e Chirurgia articolati, per le attività nel LURM, in gruppi di ricerca/assistenza riferibili a UOC afferenti a diversi Dipartimenti ad Attività Integrata (DAI). È	Misure di sicurezza ENISA	Identificazione chiara, tramite mezzi appropriati, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, con appropriati controlli di accesso per le zone definite sicure.	Applicata
		Utilizzo di sistemi antincendio automatico, sistemi di climatizzazione dedicati e di gruppi di continuità (UPS) nelle sale server.	Applicata
	Misure di sicurezza fisiche	Presenza di sistemi di videosorveglianza/controllo da parte di personale autorizzato	Applicata
		Chiusura a chiave dei locali	Applicata

Inserito nel Dipartimento di Direzione Medica Ospedaliera. Nel LURM vengono svolte attività di ricerca medica e di diagnostica avanzata. L'attività di ricerca è prevalentemente di tipo traslazionale, con impatto diretto sull'attività clinica ed attrae finanziamenti da parte di Enti nazionali ed internazionali. Le attività proprie del Centro si configurano come attività di supporto alla ricerca e alla diagnostica. L'accorpamento di più laboratori con interessi		Presenza di sistemi antincendio	Applicata

7.2 Valutazione del rischio

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Compromissione delle credenziali di accesso	Minacce in ambito di ricerca: applicativo REDCap	Riservatezza	Umano
Descrizione			
Acquisizione non autorizzata di username e password per accesso alla piattaforma REDCap da parte di soggetti non autorizzati			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza organizzative	Esistenza di una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	Esistenza di controlli periodici sulle utenze rilasciate al fine di garantirne la coerenza.	Applicata	Applicata
Misure di sicurezza tecniche	Assegnazione e gestione dei privilegi di accesso secondo il principio del privilegio minimo (Profilazione)	Applicata	Applicata
	Esistenza di regole sul corretto utilizzo e gestione della password di accesso, con obbligo di utilizzo di credenziali di elevata robustezza	Applicata	Applicata

	Accesso ai sistemi con autenticazione forte (es. MFA/CNS/smart card/certificato/firma digitale)	Applicata	Applicata
	Timeout delle sessioni dopo N minuti di inattività	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	
Totale		Totale	

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Abuso di privilegi amministrativi	Minacce in ambito di ricerca: applicativo REDCap	Riservatezza	Umano
Descrizione			
Utilizzo improprio dei privilegi di amministratore per accedere a dati non autorizzati o modificare configurazioni di sicurezza			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		2	Poco probabile
Livello di rischio iniziale		6	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza organizzative	Esistenza di procedure di formazione del personale in materia di protezione dati, compresi i profili di sicurezza	Applicata	Applicata
Misure di sicurezza tecniche	Implementazione di un sistema di audit log e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	
Totale		Totale	

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Corruzione dei dati nel Database	Minacce in ambito di ricerca: applicativo REDCap	Integrità	Umano
Descrizione			
Alterazione non autorizzata dei dati sanitari contenuti nel database REDCap compromettendo l'integrità della ricerca			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		2	Poco probabile
Livello di rischio iniziale		2	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza ENISA	Applicazione di tecniche che supportano la privacy a livello di database, come le authorized queries, il privacy preserving data base querying, la searchable encryption, ecc.	Applicata	Applicata
	Definizione di documentate procedure di backup e ripristino dei dati.	Applicata	Applicata
Misure di sicurezza tecniche	Validazione dell'input a livello di applicazione (SQL Injection)	Applicata	Applicata
	Cifratura della base dati	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile

Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Attacchi malware alla piattaforma REDCap	Minacce in ambito di ricerca: applicativo REDCap	Disponibilità ; Integrità	Umano
Descrizione			
Attacchi volti a rendere inaccessibile la piattaforma REDCap o a cifrare in maniera malevola i dati			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza ENISA	Definizione di documentate procedure di backup e ripristino dei dati.	Applicata	Applicata
Misure di sicurezza organizzative	Esistenza di procedure di formazione del personale in materia di protezione dati, compresi i profili di sicurezza	Applicata	Applicata
Misure di sicurezza tecniche	Utilizzo di protocolli di rete sicuri per l'uso dell'applicativo, usando protocolli crittografici (SSL/TLS)	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	
Totale		Totale	

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Data breach del database REDCap	Minacce in ambito di ricerca: applicativo REDCap	Riservatezza	Umano
Descrizione			
Esfiltrazione non autorizzata di dati sanitari pseudonimizzati dal database REDCap			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza ENISA	Definizione di documentate procedure di backup e ripristino dei dati.	Applicata	Applicata
Misure di sicurezza organizzative	Esistenza di procedure di formazione del personale in materia di protezione dati, compresi i profili di sicurezza	Applicata	Applicata
	Conservazione chiave di decodifica Descrizione: Conservazione in maniera sicura e separata della chiave di decodifica	Applicata	Applicata
Misure di sicurezza tecniche	Pseudonimizzazione dei dati	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve

Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Violazione della pseudonimizzazione	Minacce in ambito di ricerca: applicativo REDCap	Riservatezza	Umano
Descrizione			
Compromissione del sistema di codifica automatica permettendo la reidentificazione degli interessati			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		2	Poco probabile
Livello di rischio iniziale		6	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza organizzative	Esistenza di procedure di formazione del personale in materia di protezione dati, compresi i profili di sicurezza	Applicata	Applicata
	Conservazione chiave di decodifica Descrizione: Conservazione in maniera sicura e separata della chiave di decodifica	Applicata	Applicata
Misure di sicurezza tecniche	Assegnazione e gestione dei privilegi di accesso secondo il principio del privilegio minimo (Profilazione)	Applicata	Applicata
	Pseudonimizzazione dei dati	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve

Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Intercettazione dati durante la trasmissione	Minacce in ambito di ricerca: applicativo REDCap	Riservatezza	Contesto ; Strumenti
Descrizione			
Intercettazione non autorizzata dei dati durante la comunicazione tra client e server REDCap			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza tecniche	Canali di trasmissione protetti Descrizione: Utilizzo di canali di trasmissione protetti, tenendo conto dello stato dell'arte della tecnologia, e garantiscano, previa verifica, l'identità digitale del server che eroga il servizio e della postazione client da cui si effettua l'accesso ai dati, ricorrendo a certificati digitali emessi in conformità alla legge da un'autorità di certificazione	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile

Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Accesso non autorizzato ai file Excel con chiavi di decodifica	Minacce in ambito di ricerca: file Excel con chiavi di decodifica	Riservatezza	Umano ; Contesto
Descrizione			
Accesso non autorizzato ai file Excel contenenti le associazioni tra codici pseudonimizzati e identità reali			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		2	Poco probabile
Livello di rischio iniziale		6	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza logiche	Accesso a strumenti di lavoro per la produttività individuale tramite credenziali forti di autenticazione	Applicata	Applicata
Misure di sicurezza organizzative	Accesso alle risorse sulla base di profili di autorizzazione decisi in funzione della qualifica dell'utente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilita dall'Amministrazione	Applicata	Applicata
	Rilascio di adeguate istruzioni in merito al trattamento dei dati personali a tutti i soggetti coinvolti nella procedura	Applicata	Applicata

	Attribuzione di specifici compiti e funzioni connessi al trattamento dei dati personali a soggetti espressamente designati	Applicata	Applicata
Misure di sicurezza tecniche	Assegnazione e gestione dei privilegi di accesso secondo il principio del privilegio minimo (Profilazione)	Applicata	Applicata
	Esistenza di regole sul corretto utilizzo e gestione della password di accesso, con obbligo di utilizzo di credenziali di elevata robustezza	Applicata	Applicata
	Assegnazione ad ogni utente di chiavi di cifratura personali	Applicata	Applicata
	Cifratura della base dati	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	
Totale		Totale	

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Corruzione/alterazione delle chiavi di decodifica	Minacce in ambito di ricerca: file Excel con chiavi di decodifica	Integrità	Umano
Descrizione			
Modifica non autorizzata o accidentale dei file Excel compromettendo la possibilità di reidentificazione dei soggetti interessati			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		2	Poco probabile
Livello di rischio iniziale		2	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza ENISA	Definizione di documentate procedure di backup e ripristino dei dati.	Applicata	Applicata
Misure di sicurezza tecniche	Creazione almeno settimanalmente di una copia di sicurezza (backup) necessaria al ripristino del sistema.	Applicata	Applicata
	Garanzia di immutabilità delle copie di sicurezza.	Applicata	Applicata

	Firma digitale della base dati con hash Descrizione: Al fine di garantire l'esattezza dei dati conservati sui file Excel, in particolare a quelli afferenti ai pazienti arruolati, i fogli Excel verranno firmati digitalmente attraverso un hash. La firma digitale generata sarà detenuta da un soggetto distinto da quello addetto alla raccolta dati e verrà, nel caso, ripetuta ove i dati vengano modificati o esportati su altri file. Tale misura consente di rafforzare le tutele volte a garantire l'esattezza dei dati e ad assicurare, altresì, che eventuali successive alterazioni degli stessi siano rapidamente rilevate e corrette.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	
Totale		Totale	

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Perdita dei file dei File Excel con chiavi di decodifica	Minacce in ambito di ricerca: file Excel con chiavi di decodifica	Riservatezza	Umano
Descrizione			
Perdita dei file contenenti le chiavi di decodifica rendendo impossibile la reidentificazione			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		2	Poco probabile
Livello di rischio iniziale		2	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza ENISA	Definizione di documentate procedure di backup e ripristino dei dati.	Applicata	Applicata
Misure di sicurezza organizzative	Rilascio di adeguate istruzioni in merito al trattamento dei dati personali a tutti i soggetti coinvolti nella procedura	Applicata	Applicata
	Attribuzione di specifici compiti e funzioni connessi al trattamento dei dati personali a soggetti espressamente designati	Applicata	Applicata
Misure di sicurezza tecniche	Assegnazione e gestione dei privilegi di accesso secondo il principio del privilegio minimo (Profilazione)	Applicata	Applicata

	Creazione almeno settimanalmente di una copia di sicurezza (backup) necessaria al ripristino del sistema.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	
Totale		Totale	

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Violazione della integrità/disponibilità /tracciabilità durante il trasporto dei campioni biologici	Minacce in ambito di ricerca: trasporto materiale biologico	Disponibilità ; Riservatezza ; Integrità	Umano
Descrizione			
Smarrimento o danneggiamento del materiale biologico durante le fasi di trasporto tra centri partecipanti/promotore o tra promotore/centri partecipanti o laboratori esterni			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		2	Medio
Probabilità		1	Improbabile
Livello di rischio iniziale		2	Basso
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		2	Medio
Probabilità		1	Improbabile
Livello di rischio finale		2	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	
Nessuna		Nessuna	

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Accesso non autorizzato ai locali di conservazione	Minacce in ambito di ricerca: materiale biologico gestito presso il titolare del trattamento	Riservatezza	Umano
Descrizione			
Personale non autorizzato che accede ai laboratori, depositi e aree di conservazione del materiale biologico			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza fisiche	Presenza di sistemi antincendio	Applicata	Applicata
	Sistemazione della documentazione in contenitori (armadi, schedari, ecc.) muniti di serratura	Applicata	Applicata
	Chiusura a chiave dei locali	Applicata	Applicata
	Presenza di sistemi di videosorveglianza/controllo da parte di personale autorizzato	Applicata	Applicata
Misure di sicurezza organizzative	Rilascio di adeguate istruzioni in merito al trattamento dei dati personali a tutti i soggetti coinvolti nella procedura	Applicata	Applicata

	Attribuzione di specifici compiti e funzioni connessi al trattamento dei dati personali a soggetti espressamente designati	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	
Totale		Totale	

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Sottrazione di Campioni Biologici	Minacce in ambito di ricerca: materiale biologico gestito presso il titolare del trattamento	Disponibilità ; Integrità	Umano
Descrizione			
Sottrazione fisica di campioni biologici da parte di personale interno o esterno non autorizzato			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza fisiche	Presenza di sistemi antincendio	Applicata	Applicata
	Sistemazione della documentazione in contenitori (armadi, schedari, ecc.) muniti di serratura	Applicata	Applicata
	Chiusura a chiave dei locali	Applicata	Applicata
	Presenza di sistemi di videosorveglianza/controllo da parte di personale autorizzato	Applicata	Applicata
Misure di sicurezza organizzative	Rilascio di adeguate istruzioni in merito al trattamento dei dati personali a tutti i soggetti coinvolti nella procedura	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve

Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Scambio/Confusione di campioni	Minacce in ambito di ricerca: materiale biologico gestito presso il titolare del trattamento	Disponibilità ; Integrità	Umano
Descrizione			
Errore o sabotagio nell'identificazione che porta alla confusione tra diversi campioni biologici, compromettendo l'affidabilità della ricerca			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Misure di sicurezza fisiche	Sistemazione della documentazione in contenitori (armadi, schedari, ecc.) muniti di serratura	Applicata	Applicata
Misure di sicurezza organizzative	Esistenza di procedure di formazione del personale in materia di protezione dati, compresi i profili di sicurezza	Applicata	Applicata
	Rilascio di adeguate istruzioni in merito al trattamento dei dati personali a tutti i soggetti coinvolti nella procedura	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile

Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

Riassunto ed esito dell'analisi del rischio

Minaccia	Rischio iniziale	Rischio residuo
Compromissione delle credenziali di accesso	4	1
Abuso di privilegi amministrativi	6	1
Corruzione dei dati nel Database	2	1
Attacchi malware alla piattaforma REDCap	4	1
Data breach del database REDCap	4	1
Violazione della pseudonimizzazione	6	1
Intercettazione dati durante la trasmissione	4	1
Accesso non autorizzato ai file Excel con chiavi di decodifica	6	1
Corruzione/alterazione delle chiavi di decodifica	2	1
Perdita dei file dei File Excel con chiavi di decodifica	2	1
Violazione della integrità/disponibilità /tracciabilità durante il trasporto dei campioni biologici	2	2
Accesso non autorizzato ai locali di conservazione	1	1
Sottrazione di Campioni Biologici	1	1
Scambio/Confusione di campioni	1	1

Livello di rischio complessivo per area

Area di impatto	Livello di rischio

Riservatezza	Basso
Integrità	Basso
Disponibilità	Basso

Livello di rischio complessivo residuo

Basso

8. Coinvolgimento delle parti interessate

Domanda	**Risposta**
Sono state raccolte le opinioni degli interessati o dei loro rappresentanti?	Sì
Considerato che la valutazione del rischio risulta bassa, grazie alle misure tecniche e organizzative adottate dal titolare del trattamento, non si è ritenuto necessario coinvolgere gli interessati contattabili.	
È stato coinvolto il Responsabile della Protezione dei Dati?	Sì
Considerato che la valutazione del rischio risulta bassa, grazie alle misure tecniche e organizzative adottate dal titolare del trattamento, richiamando quanto previsto dall'art. 39 parg.1 lett. c), non si è ritenuto necessario coinvolgere il Responsabile della Protezione dei Dati aziendale come da accordi intercorsi con lo stesso.	

9. Note

Il presente documento è stato:
Redatto da: dott. Ilaria Del Giglio dell'Ufficio Privacy, coadiuvata, per la parte tecnica dal dott. Tommaso Zanardi dei Sistemi Informativi, per la parte di competenza dell'UOC REUMATOLOGIA prof. Maurizio Rossini per la parte di competenza dell'Unità di Ricerca Clinica dalla dott.ssa Silvia Martini.
Validato da:
- dott. Felice Schena, responsabile dell'Ufficio Privacy
- ing. Alessandro Manganotti, Responsabile dell'UOC Sistemi Informativi;
- prof. Maurizio Rossini, Direttore UOC Reumatologia;
- dott.ssa Anna Fratucello, Direttrice dell'UOS Unità di Ricerca Clinica.
Approvato da: Direttore Generale, quale legale rappresentante dell'Azienda titolare del trattamento.