



Azienda ospedaliero-universitaria Senese

2025

Valutazione di impatto (DPIA)

Controllo versione e Cronologia modifiche			
Versione	Data	Approvato da	Descrizione delle modifiche effettuate
1.0	07/02/2024		Prima stesura
1.1	03/06/2024		Integrazioni
1.2	04/06/2024		Revisione con ufficio privacy
Audience e distribuzione			
Strutture e Dipartimenti	Tutti		
Processo interessato	Gestione della compliance		
Livello di riservatezza documento	☐ Riservato - Documento interno ☒ ESTRATTO Pubblicabile		

Redazione Valutazione di impatto (DPIA) - Informazioni necessarie

Al fine di poter effettuare correttamente la Valutazione di impatto (DPIA) relativa ad uno specifico trattamento, come previsto dall'attuale disciplina sulla protezione dei dati personali (art. 35 GDPR), è necessario fornire le informazioni e la documentazione di seguito riportate.

NOTA: i campi con riportato l'asterisco (*) sono obbligatori; l'assenza di uno o più degli elementi obbligatori potrebbe comportare l'impossibilità di procedere alla gestione della richiesta.

Titolo del Progetto di ricerca *	"Studio retrospettivo osservazionale sul ruolo della profilassi con Fluorochinoloni nell'incidenza di infezioni batteriche nei pazienti sottoposti ad AUTOTrapianto di cellule staminali emopoietiche (studio FLAUTO)"		
Codice del Progetto di ricerca	ES_FLAUTO		
Identificativo	Nominativo *	e-mail *	Tel. (diretto/mobile) *
Responsabile del Progetto di ricerca (PI) *	Prof.ssa Monica Bocchia	m.bocchia.u@ao-siena.toscana.it ;	0577-586798
Referenti (soggetti interni alla Struttura competente per materia, ad es., funzionario, RUP, incaricato del procedimento/ trattamento dei dati personali)	1) Dott.ssa Monica Tozzi (Co-sperimentatore) 2) Dott.ssa Adele Santoni (Co-sperimentatore) 3) Dott.ssa Margherita Machiodi (Co-sperimentatore) 4) Dott.ssa Irene Bernareggi (Gestore della banca dati della ricerca).	1)m.tozzi@ao-siena.toscana.it; 2) margherita.malchiodi@ao-siena.toscana.it ; 3) adele.santoni@ao-siena.toscana.it ; 4) i.bernareggi@student.unisi.it ;	0577-586798
Definizione del trattamento			
Descrizione del Progetto di ricerca *	Riportare una breve descrizione del trattamento con indicazione del <u>flusso delle informazioni</u>, delle eventuali <u>interconnessioni</u> con altri titolari (strutture ospedaliere o enti di ricerca) o della delega ai Responsabili delle attività di trattamento: Studio clinico osservazionale e retrospettivo, multicentrico, non commerciale (no-profit). Raccolta retrospettiva di dati relativi a pazienti consecutivi (presso ogni Centro aderente allo studio) affetti da Mieloma Multiplo o Linfoma, che hanno ricevuto un trapianto autologo di cellule staminali ematopoietiche associato o meno a profilassi antibatterica o antifungina secondo la pratica clinica quotidiana dal gennaio 2016 al dicembre 2024.		
Normativa di riferimento	Leggi nazionali e regionali, Regolamenti, Atti amministrativi, Direttive, Circolari: - Regolamento (UE) 679 del 2016 - D.LGS 196 del 2003 e s.m.i - Deliberazione n.52 del 24 luglio 2008 – Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali (Pubblicato sulla Gazzetta Ufficiale n. 190 del 14 agosto 2008) - Provvedimento n. 467 dell'11 ottobre 2018 - Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018)		

Definizione del trattamento			
		- Provvedimento n. 515 del 19 dicembre 2018 - Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 (Pubblicate sulla Gazzetta Ufficiale n. 11 del 14 gennaio 2019) - Provvedimento n. 146 del 5 giugno 2019 – Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d. lgs. 10 agosto 2018, n. 101 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 176 del 29 luglio 2019) - FAQ del Garante del 06/06/2024 (https://www.garanteprivacy.it/temi/sanita-e-ricerca-scientifica/irccs)	
Area geografica del progetto di ricerca *	<i>Indicare l'estensione geografica del progetto di ricerca (in termini di soggetti coinvolti o posizionamento dei sistemi di conservazione delle informazioni):</i>	☒ nazionale; ☐ paesi dell'Unione Europea; ☐ internazionale (paesi con "decisione di adeguatezza"); ☐ soggetti sottoposti al Data Privacy Framework; ☐ internazionale (paesi non allineati ai principi del GDPR).	
Studio spontaneo o sponsorizzato *	<i>Specificare la tipologia dello studio clinico:</i>	☒ spontaneo (<i>no profit</i>); ☐ sponsorizzato (<i>profit</i>).	
Altri partecipanti al progetto	<i>Indicare denominazione e ruolo di eventuali partner (centri partecipanti), enti, sponsor o finanziatori:</i>	<i>Denominazione:</i> 1) AOUS UOC Ematologia Siena (Prof.ssa Monica Bocchia) 2) AOU Careggi (Dott.ssa Nozzoli Chiara - Dott.ssa Gozzini Antonella) 3) UOC Ematologia e Trapianti AOUP (Prof.ssa Sara Galimberti)	<i>Ruolo:</i> 1) Centro Coordinatore 2-3) centro partecipante
Tipologia di studio clinico *	<i>Specificare la tipologia di studio clinico classificato secondo la metodologia sperimentale utilizzata:</i>	<i>Studio osservazionale:</i> ☐ longitudinale prospettico; ☒ longitudinale retrospettivo; ☐ caso-controllo (anche nidificati); ☐ trasversale (studio di prevalenza); ☐ di correlazione geografica o temporale; ☐ descrittivo - serie di casi; ☐ descrittivo - studi ecologici; ☐ descrittivo - distribuzione spaziale; ☐ descrittivo - andamento temporale.	
		<i>Studio sperimentale:</i> ☐ Trial sul campo; ☐ Trial di interventi di comunità; ☐ Trial controllati randomizzati: sperimentazioni cliniche.	
Dimensione dello studio clinico *	<i>Specificare la dimensione dello studio:</i>	☐ Studio monocentrico ☒ Studio multicentrico	

Definizione del trattamento			
Autorizzazione del Comitato Etico competente	<i>Specificare se il Comitato Etico (regionale/ di altra regione) competente ha o meno valutato il progetto:</i>	☒ approvato da un Comitato Etico; ☐ presentato al Comitato Etico; ☐ valutazione preliminare da presentare al Comitato Etico.	
Modalità di arruolamento	<i>Specificare la modalità di arruolamento:</i>	☒ da parte del personale sanitario che ha in cura il soggetto; ☐ tramite associazioni; ☐ altro (<i>specificare</i>):	
Modalità di acquisizione dei dati *	<i>Specificare le modalità di raccolta dei dati personali:</i>	☐ questionari cartacei o interviste; ☐ gruppo di discussione (<i>focus group</i>); ☐ raccolta di diari (<i>diary keeping</i>); ☒ raccolta da cartella clinica; ☐ osservazione comportamentale diretta; ☐ osservazione comportamentale indiretta (a loro insaputa o tramite registrazioni audio o video); ☐ somministrazione di stimoli, compiti o procedure e registrazione di risposte comportamentali, opinioni o giudizi; ☐ somministrazione di stimoli, compiti o procedure che il soggetto potrebbe trovare fastidiosi, stressanti, fisicamente o psicologicamente dolorosi, sia durante la conduzione dello studio sia successivamente; ☐ registrazione di movimenti; ☐ immersione in ambienti di realtà virtuale; ☐ registrazione di potenziali evocati; ☐ somministrazione di test, questionari o protocolli sperimentali attraverso delle piattaforme web o posta elettronica; ☐ utilizzo di test neuropsicologici, misure elettrofisiologiche e tecniche di neuro immagine; ☐ altro (<i>specificare</i>):	
Tipologia dei soggetti invitati	<i>Specificare la tipologia di soggetti invitati a partecipare allo studio clinico e successivamente arruolati:</i>	☒ maggiorenni; ☐ minorenni; ☒ soggetti con patologie oncologiche; ☐ soggetti con disabilità fisica e psichica o con limitata capacità d'intendere o volere; ☐ soci, associati, aderenti o iscritti a organizzazioni a carattere religioso, politico, filosofico o sindacale; ☐ condannati, detenuti, imputati, indagati o sottoposti a misure di sicurezza o prevenzione; ☐ soggetti a maggiore tutela dell'anonimato (<i>vittime di atti di violenza sessuale o di pedofilia, con infezione da HIV o dediti all'uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato, presi in carico dai consultori familiari</i>).	
Numerosità degli arruolati *	<i>Specificare il numero indicativo previsto di soggetti invitati a partecipare allo studio clinico:</i>	<i>In azienda:</i> ipotizzati 300 soggetti adulti	<i>Generali:</i> ipotizzati 800 soggetti adulti (compresi i soggetti AOUS)

Definizione del trattamento		
Caratteristiche	<i>Specificare le caratteristiche del gruppo di soggetti invitati a partecipare allo studio clinico:</i>	Criteri di inclusione: ☒ età; ☐ genere; ☐ area geografica di provenienza o di residenza; ☐ appartenenza etnica; ☐ fattori di rischio cui sono esposti; ☒ altro (specificare): 1. Pazienti con diagnosi di Mieloma Multiplo o di Linfoma candidabili a trapianto autologo di cellule staminali ematopoietiche 2. Aver ricevuto un trapianto autologo di cellule staminali ematopoietiche con o senza profilassi antibatterica e antifungina. 3. Età ≥ 18 anni.
		Eventuali criteri di esclusione: 1. Soggetti di età inferiori a 18 anni. 2. Pazienti che non hanno effettuato il trapianto di cellule staminali ematopoietiche.
Rischi per gli arruolati	<i>Specificare eventuali rischi per gli arruolati allo studio clinico</i>	☐ posizione di dipendenza nei confronti del ricercatore; ☐ rischi sociali, legali o economici; ☐ intrusività degli strumenti; ☐ affaticamento; ☐ forte tensione emotiva, stress, ansia e sofferenza psicologica; ☐ possibile induzione di sentimenti di frustrazione o autosvalutazione; ☐ altro (specificare):
Data Management	<i>Indicare se è stato effettuato un Data Management Plan:</i>	☐ Documento (Plan) redatto e completato allegato al progetto (da allegare alla documentazione). ☒ Attività descritta nel protocollo del progetto
Misure di protezione dati arruolati *	<i>Specificare le previste modalità di protezione dei dati personali degli arruolati:</i>	☒ pseudonimizzazione (ad es., supporto cartaceo con elenco di decodifica); ☒ adozione di tecniche crittografiche (ad es., password su MS-Excel relativi ai dati arruolati e/o codifiche degli arruolati); ☒ piattaforma informatica per la gestione completa dello studio clinico; ☒ altro (specificare): misure ulteriori descritte nel protocollo

Motivo di redazione della DPIA	
Motivo di redazione della DPIA *	<i>Ai fini di una valutazione approfondita in ordine alla necessità di redazione della DPIA si richiamano altresì i criteri contenuti nell'Allegato 1 al provvedimento dell'Autorità Garante Privacy (GPDP) n. 467 dell'11 ottobre 2018 [doc. Web n. 9058979], di seguito riportati:</i> ☐ 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".

Motivo di redazione della DPIA

- ☐ 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).
- ☒ 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.
- ☐ Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): 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).
- ☐ Trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
- ☒ Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
- ☐ 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) ogniquale volta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .
- ☐ Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
- ☐ 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).
- ☒ Trattamenti di categorie particolari di dati ai sensi dell’art. 9 GDPR oppure di dati relativi a condanne penali e a reati di cui all’art. 10 GDPR interconnessi con altri dati personali raccolti per finalità diverse.
- ☐ Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento;
- ☐ Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento.

Requisiti minimi *

Informativa privacy * (artt. 12, 13, 14)	<i>Fornire in allegato l’informativa verticalizzata sul trattamento oggetto di DPIA, completa e/o in formato breve (ad esempio, riportata nella modulistica o pubblicata in piattaforma online):</i>	<i>Modalità di ostensione prevista:</i> ☒ sito web istituzionale/dedicato; ☐ piattaforma online dedicata al trattamento; ☒ fornita direttamente al singolo interessato; ☐ altro (specificare):
Nomina soggetti	<i>I soggetti deputati al trattamento</i>	<i>Modalità di autorizzazione:</i>

Requisiti minimi *		
autorizzati *	<i>devono essere specificatamente autorizzati:</i>	☒ nomina singolo soggetto autorizzato; ☐ nomina funzionale per appartenenza alla struttura/UO competente.
Soggetti coinvolti nel trattamento dei dati personali	<i>Ruolo dell'Azienda nello studio clinico:</i>	☒ Titolare ☐ Contitolare ☐ Responsabile / Sub-Responsabile
	<i>Titolari:</i>	1) AOU Careggi di Firenze 2) AOU Pisana
	<i>Contitolari:</i>	
	<i>Responsabili dell'Azienda:</i>	☒ Estar ☐ altri (specificare):
	<i>Sub-Responsabili</i>	☒ fornitori di applicativi e software (nominati da ESTAR ☐ altro (specificare)
Nomina Responsabili da parte dell'azienda *	<i>I soggetti giuridici che effettuano attività in outsourcing (fornitori, gestori di servizi, ecc.) devono essere nominati con accordo ai sensi dell'art. 28 GDPR rispetto allo specifico trattamento, integrando istruzioni documentate, con adeguato obbligo legale di riservatezza del personale impiegato nel trattamento, adottando le misure di sicurezza tecniche e organizzative necessarie rispetto alla tipologia di dati trattati e ai rischi incombenti:</i>	<i>Modalità di nomina:</i> ☐ Contestualmente alla firma del contratto/ convenzione/protocollo d'intesa; ☒ Protocollo n° 7314 del 2024 per ESTAR; ☒ Non sono delegate ad altri soggetti terzi attività di trattamento di dati personali; ☐ Altro (specificare):
Analisi del Rischio	<i>L'analisi del rischio deve essere effettuata in via propedeutica rispetto alla DPIA – attraverso il <u>modello di "Analisi Rischi"</u> allegato nel caso di numerosità di arruolati elevata o su trattamenti di dati personali critici - ed il relativo esito in termini di "LIVELLO DI RISCHIO COMPLESSIVO" deve essere "ACCETTABILE". Nel caso in cui il livello complessivo di rischio risulti "NON ACCETTABILE", si dovrà procedere con l'adozione di ulteriori misure tecniche e organizzative previste dal modello fino ad arrivare alla accettabilità del rischio [livello di rischio "ACCETTABILE"]. La suddetta analisi del rischio va obbligatoriamente allegata alla DPIA:</i>	Risultato dell'Analisi del rischio: ☒ ACCETTABILE

Elementi necessari per la valutazione dei rischi * (<i>indicare almeno una delle tre tipologie contemplate</i>)		
Piattaforme informatiche utilizzate nel trattamento	Riportare gli indirizzi web (URL) delle piattaforme informatiche utilizzate, sia regionali che esterne al perimetro di sicurezza (ad es., <a href="https://<xyz>.com">https://<xyz>.com):	piattaforma Red Cap: https://aous-redcap.unisi.it/
Asset utilizzati	Indicare gli altri applicativi software utilizzati (ad esempio, software installati localmente o condivisioni di rete, file hosting, ecc.):	cartella clinica informatizzata aziendale e applicativi di supporto
	Indicare i sistemi o dispositivi hardware utilizzati (portatili, tablet, smartphone, dispositivi wearable, Internet of Things, ecc.):	PC aziendali
Supporti cartacei	Indicare le modalità di trattamento su supporto cartaceo effettuate, inclusa la conservazione:	documenti sanitari

Valutazione di impatto (DPIA) - Informazioni generali			
Operazioni effettuate sui dati personali: *	☒ raccolta	☒ registrazione	☒ organizzazione
	☒ conservazione	☒ adattamento	☒ modifica
	☒ consultazione	☒ comunicazione	☒ trasmissione
	☒ messa a disposizione	☒ raffronto	☐ interconnessione
	☒ cancellazione	☒ distruzione	
Dati personali *	Indicare le macrocategorie di dati personali trattati:	☒ Dati comuni (nominativo, indirizzo, e-mail, telefono, , ecc.); ☒ Dati particolari [art. 9 GDPR] ☐ Origine razziale o etnica; ☐ Opinioni politiche; ☐ Convinzioni religiose o filosofiche; ☐ Appartenenza sindacale; ☐ Dati genetici; ☐ Dati biometrici; ☒ Dati relativi alla salute; ☐ Dati relativi alla vita sessuale; ☐ Dati relativi all'orientamento sessuale; ☐ Dati di soggetti a maggiore tutela dell'anonimato (relativi ad atti di violenza sessuale o di pedofilia, all'infezioni da HIV o all'uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, alle prestazioni erogate alle donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato e ai servizi offerti dai consultori familiari) ["Linee guida in materia di dossier sanitario" - Allegato A alla deliberazione del Garante Privacy del 4 giugno 2015; art. 6, D.M. Ministro della Salute del 7.9.2023 - "Fascicolo Sanitario Elettronico 2.0"]; ☐ Dati giudiziari [art. 10 GDPR].	
	EsPLICITARE ulteriori tipologie di dati personali trattati:	☐ famiglia o situazioni personali; ☐ lavoro (occupazione attuale e precedente, curriculum, ecc.); ☐ istruzione e cultura (diploma, laurea, attestati, ecc.); ☐ altro (specificare):	
Natura del trattamento	Indicare eventuali caratteristiche intrinseche del trattamento che possano rappresentare un rischio rilevante per gli interessati	☐ processo decisionale automatizzato; ☐ rapporti di forza asimmetrici; ☐ imprevedibilità del trattamento (ad es., IA); ☐ difficoltà per l'interessato di esercitare i propri diritti; ☐ altro (specificare):	

	[EDPB guidelines 201904 data protection by design and by default v2.0]:	
Modalità di trattamento	Specificare le previste modalità di trattamento dei dati personali:	☒ utilizzo di un solo strumento di conservazione ed elaborazione per tutta la durata dello studio e del ciclo di vita delle informazioni; ☒ <i>screening</i> (selezione dei partecipanti idonei alla ricerca); ☐ assegnazione randomizzata dei partecipanti ai gruppi di sperimentazione; ☐ somministrazione trattamenti farmacologici; ☒ <i>follow up</i> - assistenza e monitoraggio; ☐ verifica periodica del rispetto del protocollo di ricerca; ☐ effettuate analisi di tipo <i>big data</i> (multipli <i>dataset</i> o combinazione e analisi di differenti <i>dataset</i>); ☐ implementazione di tecnologie di IA nell'analisi dei dati; ☐ calcolo automatico di un punteggio relativo ad aspetti o comportamenti di un individuo; ☐ profilazione (quando la finalità è la valutazione delle caratteristiche individuali dei soggetti).
Valutazione delle misure atte a garantire necessità e proporzionalità del trattamento [art. 35, paragrafo 7, lettera b) GDPR]		
Finalità *	Descrivere le finalità del trattamento:	☒ ricerca scientifica e statistica; ☒ ricerca medica, biomedica ed epidemiologica; ☐ altro (<i>specificare</i>):
Condizioni di liceità del trattamento *	Indicare la base giuridica ai sensi degli art. 6 GDPR relativamente ai dati personali comuni :	☒ consenso dell'interessato [art. 6, par. 1, lett. a) GDPR]; ☐ obbligo legale [art. 6, par. 1, lett. c) GDPR] (solo nel caso di norme specifiche o prescrizioni ministeriali); ☐ compito di interesse pubblico o connesso all'esercizio di pubblici poteri [art. 6, par. 1, lett. e) GDPR]; ☒ requisiti previsti dall'art. 110 D.lgs. 196/03 per pazienti deceduti o non contattabili.
	Indicare la base giuridica ai sensi dell'art. 9 GDPR relativamente alle particolari categorie di dati personali (ex dati sensibili)	☒ consenso dell'interessato [art. 9, par. 2, lett. a) GDPR]; ☐ trattamento necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali [art. 9, par. 2, lett. h) GDPR]; ☐ trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici [art. 9, par. 2, lett. i) GDPR]; ☒ requisiti previsti dall'art. 110 D.lgs. 196/03 per pazienti deceduti o non contattabili.
Adeguatezza, pertinenza e non eccedenza (art. 5, par. 1, lettera c) GDPR)	Indicare le misure poste in essere al fine di garantire adeguatezza (efficacia della protezione dei dati):	☐ sistema di gestione della sicurezza delle informazioni; ☒ analisi del rischio effettuata; ☐ applicati principi di <i>security/privacy by design</i> ; ☐ verifiche periodiche sui sistemi/piattaforme (VA/PT); ☒ controllo degli accessi (<i>need to know, need to do</i>); ☒ limitazione dell'accesso (degli operatori e rispetto ai contenuti); ☐ segregazione dell'accesso; ☒ trasferimenti protetti e sicuri;

		☒ conservazione sicura; ☒ pseudonimizzazione; ☒ backup e repliche; ☒ registrazione continua degli eventi e delle azioni (log); ☐ piano di disaster recovery/continuità operativa; ☒ procedura di data breach e risposta agli incidenti.
	<i>Indicare le misure poste in essere al fine di garantire la pertinenza (correttezza della base giuridica):</i>	☒ effettuata e mantenuta aggiornata la mappatura dei trattamenti; ☒ applicata la corretta base giuridica, validata con il DPO; ☐ base giuridica differenziata per ciascuna attività di trattamento; ☐ trattamento necessario e non soggetto a condizioni; ☐ piena autonomia dell'interessato nel controllo dei propri dati personali; ☐ base giuridica predeterminata prima dell'inizio del trattamento; ☐ cessazione del trattamento nel caso di base giuridica non più valida; ☐ adeguamento del trattamento rispetto alla eventuale modifica della base giuridica.
	<i>Indicare le misure poste in essere al fine di garantire la non eccedenza (principio di necessità), anche in logica di privacy by design:</i>	☒ i dati trattati, le funzioni e i profili di autorizzazione sono predeterminati prima dell'inizio del trattamento; ☐ i dati trattati sono stati minimizzati e validati come nucleo minimo; ☐ sono effettuate verifiche periodiche in relazione ai dati trattati, alle funzioni e ai profili di autorizzazione.
Esattezza e aggiornamento dei dati (art. 5, par. 1, lettera d) GDPR)	<i>Indicare eventuali misure poste in essere al fine di garantire esattezza e aggiornamento dei dati.</i>	☒ fonti dei dati personali affidabili (per dati acquisiti non direttamente dall'interessato); ☒ correttezza dei dati personali verificata periodicamente durante lo studio clinico; ☒ cancellazione/rettifica tempestiva dei dati su richiesta dell'interessato secondo procedura; ☐ effetto della propagazione di errori ridotto grazie ai controlli; ☒ aggiornamento dei dati da parte dell'interessato secondo prevista procedura; ☐ in fase di acquisizione sono previste soltanto scelte concise e predeterminate anziché campi a testo libero.
Periodo di conservazione dei dati personali *	<i>Indicare le tempistiche previste di conservazione dei dati personali:</i>	Numero anni (<i>specificare</i>): 4 anni <i>Fonte:</i> ☐ fonte normativa o amministrativa; ☐ massimario di conservazione aziendale; ☐ accordo con sponsor; ☒ altro (<i>specificare</i>): protocollo del progetto.
	<i>Criteri per determinare il periodo di conservazione, nel caso in cui il numero di anni non sia determinabile con esattezza o superi i 7 anni, 25 anni per la sperimentazione clinica:</i>	☐ cancellazione automatica alla conclusione del trattamento; ☐ legato a specifiche necessità e finalità (<i>specificare</i>): ☐ altro (<i>specificare</i>):
Valutazione delle misure atte a garantire i diritti degli interessati		
Esercizio dei diritti	<i>Indicare le previste modalità di esercizio dei diritti:</i>	☒ procedura di Accesso (art. 15); ☒ procedura di Rettifica (art. 16); ☒ procedura di Revoca del consenso (art. 17 pa. 1 lett. b).

Garanzie riguardanti l'eventuale trasferimento dei dati personali in Paesi terzi * (Capo V GDPR)	<i>Indicare se sono effettuati trasferimenti dei dati personali in Paesi esteri e quali misure sono poste in essere a garanzia dei diritti degli interessati (sono riportate in grassetto le misure di conformità ricorrenti):</i>	☐ Sono previsti trasferimenti di dati personali extra UE; ☒ Non sono previsti trasferimenti di dati personali extra UE. <i>In caso di trasferimenti extra UE, sono previste le seguenti misure di conformità:</i> ☐ decisioni di adeguatezza [art. 45 GDPR] ☐ strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici [art. 46, par. 2, lett. a GDPR]; ☐ norme vincolanti d'impresa o Binding Corporate Rules (BCR) [art. 46, par. 2, lett. b]; ☐ clausole tipo o contrattuali standard (SCC) [art. 46, par. 2, lett. c e lett. d]; ☐ codici di condotta [art. 46, par. 2, lett. e]; ☐ meccanismi di certificazione [art. 46, par. 2, lett. f]; ☐ consenso degli interessati [da considerarsi base giuridica residuale nell'ambito della ricerca]. <i>Previa autorizzazione del Garante:</i> ☐ clausole contrattuali ad hoc [art. 46, par. 3, lett. a]; ☐ accordi amministrativi tra autorità o organismi pubblici [art. 46, par. 3, lett. b].
Consultazione preventiva * (art. 36 GDPR)	<i>Riportare se è stata effettuata, anche precedentemente, una consultazione preventiva presso l'Autorità Garante:</i>	☐ effettuata consultazione preventiva presso l'Autorità Garante; ☒ non si è ritenuto necessario effettuare la consultazione preventiva presso l'Autorità Garante.
Altre informazioni utili alla valutazione		
Opinioni degli interessati o dei loro rappresentanti (art. 35, par. 9)		
Note	Redatta il 29.08.2025	
Data e firma dello sperimentatore principale AOUS	OMISSIS Firmato dallo sperimentatore principale in data 01/10/2025	