Prot. n. 0201684 del 07/06/2023 - UOR: 003289

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

Valutazione d'impatto

TRATTAMENTO DEI DATI INERENTI IL PROGETTO DI RICERCA IN AMBITO SANITARIO

"SUPER-CAT"

Indicazioni preliminari sulla presente DPIA

Il trattamento è stato implementato in riferimento allo studio clinico dal titolo *"Duplice terapia antiglutammatergica con Ketamina e Perampanel nello stato epilettico super-refrattario post-anossico: studio clinico osservazionale di coorte, retrospettivo, multicentrico (SUPER-CAT)"*, posto in essere al fine di valutare l'efficacia e la sicurezza della terapia combinata con ketamina e perampanel in pazienti con SE super-refrattario ad eziologia post-anossica, rispetto ad altre terapie.

Informazioni sulla DPIA

Nome della DPIA – Indicazione del Trattamento

Trattamento dei dati inerenti il progetto di ricerca in ambito sanitario "SUPER-CAT"

Nome autore

Giorgia Campanelli

Nome valutatore – operazioni di calcolo

Pasquale Ficara, Stefano Pastori

Nome validatore

Emanuela Mazzotta, RPD

Data di creazione

Marzo 2023

Cenni sulla metodologia utilizzata per la DPIA

Il presente documento è stato redatto dal Settore Legale, in qualità di Ufficio di supporto al RPD, su indicazione del responsabile, tenendo conto, oltre che del GDPR, delle Linee Guida approntate dall'Autorità Garante Italiana, dal CNIL (Autorità francese), dal WP29 – Gruppo di lavoro europeo e da ENISA.

Le linee guida sopra riportate sono state utilizzate sia per la redazione della parte descrittiva, sia per la definizione di pesi e misure per l'implementazione della parte di calcolo, basata su criteri predeterminati ed oggettivi.

Alla luce delle linee guida di cui sopra, il metodo è stato elaborato tenendo conto altresì dell'organizzazione interna dell'Ateneo e delle specifiche esigenze dell'Ente.

Contesto

Panoramica del trattamento

Qual è il trattamento in considerazione?

Lo studio si propone di raccogliere in modo retrospettivo i dati clinici di pazienti ricoverati presso il reparto di Terapia Intensiva Cardiochirurgica con una grave forma di epilessia che si può

verificare come conseguenza del danno cerebrale causato dall'arresto cardiaco, chiamata "stato epilettico super-refrattario post-anossico". Mediante la raccolta dei dati clinici che riguardano la gravità del danno cerebrale iniziale e dell'arresto cardiaco, la terapia praticata, la risoluzione o meno dello stato epilettico valutata con l'elettroencefalogramma e il suo stato di salute a distanza di 6 mesi dall'arresto cardiaco, lo studio SUPER-CAT ha lo scopo di paragonare l'efficacia e la sicurezza della terapia combinata con il farmaco anestetico ketamina e il farmaco antiepilettico perampanel, rispetto ad altre terapie antiepilettiche e anestetiche utilizzabili in questa condizione.

Finalità:

- I risultati dello studio permetteranno di confrontare la fattibilità, l'efficacia e la sicurezza della duplice terapia antiglutamaterica con ketamina e perampanel nello SE post-anossico super-refrattario rispetto ad altre terapie anti-epilettiche e anestetiche, utilizzate nella normale pratica clinica. Se clinicamente rilevanti, questi risultati permetteranno di porre le basi per lo sviluppo di un successivo trial clinico randomizzato.

Quali sono le responsabilità connesse al trattamento?

Titolare: Università degli Studi di Milano -Bicocca

RPD: Emanuela Mazzotta

Responsabile Interno: P.I. Prof. Carlo Ferrarese

Referente dell'Area: Dipartimento di Medicina e Chirurgia, nella persona del Direttore di Dipartimento, Prof. Pietro Invernizzi

Referente per il servizio: Prof.ssa Maria Grazia Valsecchi

Responsabile esterno: Società Nphase Inc per la piattaforma RedCap

Quali sono i Soggetti coinvolti nel trattamento?

Lo studio vede come:

- Promotore l'Università degli Studi di Milano-Bicocca;
- Centro Coordinatore la Fondazione IRCCS San Gerardo dei Tintori.;
- Centri partecipanti allo studio le Unità di Terapia intensiva e Rianimazione in collaborazione con le rispettive U.O. di Neurologia di 11 ospedali italiani.

I rapporti tra il Promotore e il Coordinatore sono regolati dalla Convenzione quadro formalizzata tra l'Università degli Studi di Milano-Bicocca e l'ASST Monza Ospedale San Gerardo in data 12/06/2019.

I rapporti tra il Promotore e i vari Centri partecipanti sono regolati dai singoli contratti ad hoc via via formalizzati.

Ci sono standard applicabili al trattamento?

No, trattamento implementato per la prima volta e con tecnologie recenti.

Dati, processi e risorse di supporto – Valutazione del Rischio

Quali sono i dati trattati? Apporre una x sulle categorie interessate:

CATEGORIE DI DATI PERSONALI	
Dati anagrafici (nome e cognome, data e luogo di nascita, sesso, stato civile ecc.)	X
Dati di residenza (indirizzo di residenza, domicilio, dimora)	X
Dati di contatto (telefono fisso, telefono cellulare, e-mail personale ecc.)	X
Dati finanziari (codice fiscale, codice IBAN, dichiarazione redditi, situazione patrimoniale ecc.)	
Dati particolari (orientamento sessuale, convinzioni religiose o politiche, biometrici, etnia ecc.)	
Dati giudiziari (sentenze o procedimenti penali o civili, casellario giudiziale ecc.)	
Dati genetici[1] (vedere nota)	
Dati sanitari (gravidanza, certificazioni di patologie gravi e/o invalidanti ecc.)	X

Profilo dei trattamenti ad elevato impatto – Il trattamento rientra in uno o più profili indicati nella tabella seguente?

PROFILO DEI TRATTAMENTI AD ELEVATO IMPATTO	***SÌ***	***NO***
Trattamenti che mirano a valutare il soggetto interessato, comprese la profilazione e le attività utili a fare previsioni/statistiche, in particolare relativi a: rendimento professionale, situazione economica, salute, preferenze o interessi personali, affidabilità, comportamento, ubicazione o spostamenti dell'interessato[2].		X
Decisioni/trattamenti automatizzati che producono significativi effetti giuridici o di analoga natura sulla persona fisica interessata[3].		X
Tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto. Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto.		X

[1] Dati riguardanti le caratteristiche genetiche di una persona fisica che siano ereditarie o acquisite (…) che forniscono informazioni uniche sulla fisionomia o sulla salute dell'individuo considerato, ottenuti in particolare dall'analisi di un campione biologico

[2] Esempio: una società operante nel settore delle biotecnologie che offra test genetici ai consumatori per finalità predittive del rischio di determinate patologie o in generale per lo stato di salute; una società che crei profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito web.

[3] Esempio: il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione. Il trattamento che produce effetti minimi o nulli su un interessato non soddisfa questo specifico criterio.

Dati relativi a interessati vulnerabili: tutte quelle situazioni in cui è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento, nel senso che l'interessato può non disporre del concreto potere di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti[4].	X	

Profilo dei trattamenti ad elevata probabilità di evento negativo – Il trattamento rientra in uno o più profili indicati nella tabella seguente?

PROFILO DEI TRATTAMENTI AD ELEVATA PROBABILITÀ DI EVENTO NEGATIVO	***SÌ***	***NO***
Monitoraggio sistematico: quei trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico.		X
Trattamenti di dati su larga scala: per numero di interessati al trattamento, per volume di dati trattati, per molteplicità di tipologie di dati, per notevole durata del trattamento, per ampiezza dell'ambito geografico del trattamento.		X
Combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative iniziali dell'interessato.		X
Utilizzi innovativi di mezzi/sistemi noti o applicazione di nuove soluzioni tecnologiche o organizzative, come l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici, e così via.[5]		X

Quali sono gli ambiti di impatto rispetto al trattamento?

CATEGORIE POSSIBILI AMBITI DI IMPATTO

[4] La categoria degli interessati vulnerabili comprende anche: i minori, i quali si può ritenere non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali; i dipendenti; quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti); ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.

[5] Il GDPR chiarisce che l'utilizzo di una nuova tecnologia, definito "in conformità con il grado di conoscenze tecnologiche raggiunto", può generare forme innovative di raccolta e utilizzo dei dati cui può associarsi un rischio elevato per i diritti e le libertà delle persone. Nei fatti, le conseguenze sul piano individuale e sociale del ricorso a una nuova tecnologia (o all'uso innovativo di una tecnologia conosciuta) sono a volte ignote e imprevedibili. Per esempio, alcune applicazioni legate all'"Internet delle cose" potrebbero avere impatti significativi sulla vita privata e le abitudini delle persone. Tutto ciò aumenta la probabilità che insorgano problemi.

FISICO[6]	X	*MORALE*[7]		*ECONOMICO*[8]	

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

Lo studio clinico osservazionale di coorte, retrospettivo, multicentrico coinvolgerà 11 ospedali italiani, per un totale di 80 pazienti, e verrà condotto presso le Unità di Terapia intensiva e Rianimazione in collaborazione con le rispettive U.O. di Neurologia. Lo studio avrà una durata complessiva di 18 mesi. Il periodo osservato sarà di 36 mesi.

I dati demografici e clinici verranno raccolti ed inseriti in modo pseudonimizzato in una e-CRF dedicata. I risultati dello studio permetteranno di confrontare la fattibilità, l'efficacia e la sicurezza della duplice terapia antiglutamaterica con ketamina e perampanel nello SE post-anossico super-refrattario rispetto ad altre terapie anti-epilettiche e anestetiche, utilizzate nella normale pratica clinica. Se clinicamente rilevanti, questi risultati permetteranno di porre le basi per lo sviluppo di un successivo trial clinico randomizzato.

Le principali fasi del progetto sono:

1. Arruolamento pazienti

   (Ciascun Centro Partecipante recluterà in modo retrospettivo tutti i pazienti consecutivi ospedalizzati in possesso dei criteri di idoneità dello studio. Sulla base di dati precedenti raccolti dal Centro Coordinatore nel quinquennio 2016-2020 e di una survey preliminare presso i Centri partecipanti, la frequenza di pazienti con stato epilettico super-refrattario post-anossico che presentano i criteri di inclusione dello studio è stimata di circa 2-5 pazienti/anno. Considerando le dimensioni eterogenee dei Centri partecipanti, si stima un periodo di reclutamento retrospettivo di 36 mesi per raggiungere la dimensione campionaria desiderata.)

2. Raccolta dati

   (I dati sono già stati raccolti nella cartella clinica dei soggetti che rientrano nella casistica dello studio. La raccolta dei dati è responsabilità del personale del centro coinvolto nello

[6] *La sfera fisica si riferisce a tutto ciò che attiene all'incolumità e alla sicurezza fisica della persona. Un impatto su tale sfera potrebbe verificarsi, ad esempio, nel caso di distruzione di dati clinici necessari allo svolgimento di una terapia, di dati relativi a patologie (allergie ecc.) il cui mancato o errato riscontro potrebbero non far scattare le relative misure di sicurezza/accortezza.*

[7] *Nell'ambito morale rientrano tutti gli impatti che possono pregiudicare l'onore, la reputazione, la dignità, l'immagine ecc. della persona.*

[8] *Si tratta degli impatti che producono effetti negativi sulla situazione economica della persona.*

studio clinico. Il follow-up verrà condotto tramite consultazione della cartella clinica oppure, se necessario, tramite contatto telefonico. Il follow-up verrà effettato dopo almeno 6 mesi dalla data dell'arresto cardio-circolatorio. Verrà raccolto il dato relativo all'outcome funzionale del paziente, utilizzando la scala di Rankin modificata, riferito allo stato del paziente a circa 6 mesi dall'arresto cardio-circolatorio.)

3. Inserimento dati (in forma pseudonimizzata) su eCRF e follow-up

   (Il personale del centro coinvolto nello studio, sotto la responsabilità del PI presso quel centro, estrarrà i dati di interesse e li inserirà nella eCRF in forma pseudonimizzata (ossia verrà assegnato un codice identificativo per ciascun soggetto reclutato). Solo il personale sanitario coinvolto nello studio potrà poi risalire dal codice generato, al nome del paziente. Il personale sanitario verificherà la correttezza e la completezza dei dati. Solo nel caso lo ritenga necessario i dati verranno aggiornati, quindi modificati. I dati verranno organizzati secondo la struttura della eCRF, precedentemente autorizzata dal CE competente.).

4. Analisi statistica dei dati

   (Tramite operazioni di consultazione, raffronto, inter-connessione ed elaborazione, i dati verranno esportati dalla piattaforma, in forma pseudonimizzata, e analizzati dallo statistico dello studio.)

N.B. Le suddette fasi di arruolamento retrospettivo, inserimento dati e follow-up prevedono una durata di 12 mesi

5. Conservazione e Pubblicazione risultati dello studio

   (I dati verranno conservati per tutta la durata dello studio e per un ulteriore periodo di tempo necessario affinché il Titolare o lo sperimentatore del Centro, a seconda dei casi, possano comunicare, interpretare, verificare le informazioni in modo preciso e pubblicare i risultati dello studio, tutelando al tempo stesso la riservatezza dei dati personali in conformità al regolamento UE sul trattamento dei dati personali e alla normativa nazionale in materia di trattamento dei dati personali.)

6. Distruzione dati dello studio

   (I dati verranno successivamente distrutti.)

Quali sono le risorse di supporto ai dati?

I dati verranno imputati e gestiti mediante utilizzo di CRF elettronica (eCRF) sviluppata con piattaforma REDCap Cloud e accessibile tramite specifico indirizzo url (https://eulogin.redcapcloud.com/#cid=nph2020&act=list&studyId=362).

Quali sono le modalità di trattamento rispetto alle risorse di supporto dati?

FONTI DI SUPPORTO					
UMANA INTERNA[9]	X	*UMANA ESTERNA*[10]	X	*NON UMANA - TECNICA*[11]	X

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Si, in quanto il sistema è implementato al fine di valutare l'efficacia e la sicurezza della terapia combinata con ketamina e perampanel (duplice terapia anti-glutammatergica) in pazienti con SE super-refrattario ad eziologia post-anossica, rispetto ad altre terapie.

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica è rappresentata dal protocollo di studio, che a monte richiama sia il contratto di contitolarità tra Promotore e Centro Coordinatore, sia i singoli contratti che verranno stipulati tra Promotore e Centri Partecipanti allo studio, con particolare riguardo a quanto disciplinato nell'Art. 8 Consenso informato e dall'Art. 9 Protezione dei dati personali dei pazienti.

Ulteriore base giuridica è data dal consenso al trattamento dei dati fornito da parte di tutti gli interessati coinvolti nel progetto di ricerca. Il foglio informativo ed il consenso informato verranno forniti a ciascun Centro partecipante.

Lo studio, in quanto retrospettivo, coinvolge e tratta anche i dati di soggetti per i quali risulta impossibile acquisire il consenso al trattamento in quanto trattasi di soggetti deceduti o soggetti con diagnosi di stato epilettico super refrattario post arresto cardio-circolatorio, con elevata incidenza di mortalità nelle settimane successive all'arresto cardio-circolatorio.

Qualora tale evenienza dovesse presentarsi e abbia i requisiti previsti dall'Autorizzazione generale del Garante per la Protezione dei Dati Personali al trattamento dei dati personali per scopi di ricerca scientifica 9/2016, come prorogata dal Provvedimento del Garante della Privacy n. 424 del 2018 e per il contenuto ritenuto compatibile in accordo a quanto disposto dall'art. 21 del D.Lgs. n.

[9] I soggetti a vario titolo inquadrati nell'organizzazione dell'Ateneo (dipendenti, collaboratori, studenti ecc.) che possono a vario titolo e modo, agire sui dati personali.

[10] I soggetti esterni all'Ateneo che possono a vario titolo e modo agire sui dati personali raccolti e gestiti dall'Ateneo.

[11] Sono essenzialmente gli strumenti tecnici di elaborazione informatica o di raccolta/registrazione/conservazione dei dati il cui cattivo funzionamento potrebbe causarne la distruzione, la diffusione illecita ecc.

101/2018, si potrà derogare al consenso informato al trattamento dei dati personali dei soggetti alle condizioni previste dalla suddetta autorizzazione.

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

Sì, anche per quanto rilevato dall'Autorità garante.

I dati sono esatti e aggiornati?

Si

Qual è il periodo di conservazione dei dati?

TEMPO DI CONSERVAZIONE DEL DATO							
BREVE *(meno di 1 anno)*		***MEDIO*** *(da 1 a 10 anni)*	X	***MEDIO LUNGO*** *(oltre 10 e fino a 20 anni)*		***LUNGO*** *(oltre 20 anni)*	

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Qualora possibile, con apposita informativa sul trattamento somministrata ai pazienti.

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso informato per l'inserimento dei dati verrà sottoposto al paziente, oppure ad un suo rappresentante legale, appena se ne presenterà l'occasione.

Qualora tale occasione non dovesse presentarsi per motivi di impossibilità organizzativa tali che all'esito di ogni ragionevole sforzo compiuto per contattarli, anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente, i pazienti risultino essere al momento dell'arruolamento nello studio deceduti o non contattabili, non sarà raccolto il consenso informato del paziente.

Qualora si presenti l'occasione, lo sperimentatore spiega al soggetto in cosa consiste lo studio, quali sono gli obiettivi che si pone di raggiungere, eventuali benefici per il soggetto e qualsiasi altra informazione necessaria a capire lo studio; la spiegazione deve avvenire in maniera e con un linguaggio comprensibile al soggetto e dedicando il tempo necessario affinché il soggetto comprenda a pieno lo studio e possa fare eventuali domande. Una volta terminata questa fase di colloquio, lo sperimentatore consegna il modulo di Consenso informato al soggetto che potrà decidere di firmare al momento oppure di portare a casa, valutare con calma e consegnare in un secondo momento. Una copia del Consenso e dell'Informativa Privacy resterà al paziente.

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

Ove possibile, è esercitabile il diritto di portabilità nonché il diritto di accesso nelle forme previste dal GDPR.

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

Ove possibile, è esercitabile il diritto di cancellazione nonchè il diritto alla rettifica nella denegata ipotesi di un dato non aggiornato.

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

Ove possibile, sono esercitabili tali diritti.

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

E' stata redatta la nomina a Responsabile del Trattamento nei confronti della società nPhase Inc per la piattaforma RedCap.

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

Il trasferimento dei dati al di fuori dell'Unione europea non è previsto. Ma, nel caso si verifichi tale necessità, il suddetto trasferimento avverrà esclusivamente tramite la piattaforma RedCAP cloud. Il personale clinico avrà accesso alla piattaforma RedCAP solo quando avrà letto il manuale di utilizzo fornito dal Promotore.

Rischi – Analisi per la valutazione d'impatto

Misure esistenti o pianificate

Misure di Sicurezza per struttura informatica e digitale

1. *Controllo degli accessi logici:* si
2. *Crittografia:* si
3. *Archiviazione:* si
4. *Lotta contro il malware:* si
5. *Sicurezza dei siti web:* sì
6. *Aggiornamento dell'infrastruttura tecnico-informatica:* sì
7. *Sicurezza dei canali informatici:* sì
8. *Controllo degli accessi fisici:* non pertinente
9. *Gestione delle politiche di tutela della privacy:* sì
10. *Gestione dei rischi:* sì
11. *Tracciabilità:* si, ove possibile.

Misure di Sicurezza per struttura fisica e/o supporto analogico

1. *Tracciabilità*: non pertinente

2. *Archiviazione:* non pertinente
3. *Manutenzione*: non pertinente
4. *Controllo accessi fisici*: non pertinente
5. *Gestione delle politiche di tutela della privacy*: non pertinente
6. *Gestione del rischio incendio*: non pertinente
7. *Gestione del rischio alluvione*: non pertinente
8. *Gestione del rischio altri eventi naturali distruttivi*: non pertinente

Accesso illegittimo ai dati

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

Accesso potenziale ed esfiltrazione dei dati dell'interessato.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso abusivo alla piattaforma e copiatura dati.

Quali sono le fonti di rischio?

Umana e non umana

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, sicurezza malware, aggiornamento dell'infrastruttura tecnico-informatica, sicurezza dei siti web, gestione politiche privacy, gestione del rischio.

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?

molto bassa

Modifiche indesiderate dei dati

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

Alterazione dei dati, al fine di falsare i dati clinici raccolti

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

Manomissione della piattaforma

Quali sono le fonti di rischio?

Umana e non umana

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

Crittografia, sicurezza malware, aggiornamento dell'infrastruttura tecnico-informatica

Come stimereste la gravità del rischio, in particolare 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?

Molto bassa

Perdita di dati

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

Violazione dei dati

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

Accesso abusivo, violazione dati (anche considerando la cancellazione manuale accidentale)

Quali sono le fonti di rischio?

Umana e non umana

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

Politiche di protezione del dato

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?

Molto bassa

ANALISI VALUTATIVA EFFETTI PER TIPI DI RISCHIO

Rispondere con "sì" nel caso in cui l'effetto potrebbe realizzarsi o con "no" nel caso contrario, inserendo la risposta nelle caselle corrispondenti.

	1	*Gli interessati possono far fronte alla perdita di riservatezza solo subendo impatti significativi e difficilmente risolvibili?*	Sì

PERDITA RISERVATEZZA	*2*	*A causa della perdita di riservatezza gli interessati hanno un problema economico, una perdita di opportunità o particolari minacce?*	Sì
	3	*A causa della perdita di riservatezza gli interessati hanno un importante impatto economico, impedimento di accesso a fondi e finanziamenti?*	No
	4	*A causa della perdita di riservatezza gli interessati hanno un danno irreversibile (perdita del lavoro, impatti psicologici a lungo termine, ecc.)?*	No
PERDITA INTEGRITÀ	*1*	*Gli interessati possono far fronte alla perdita di integrità solo subendo impatti significativi e difficilmente risolvibili?*	Sì
	2	*A causa della perdita di integrità gli interessati hanno un problema economico, una perdita di opportunità o particolari minacce?*	Sì
	3	*A causa della perdita di integrità gli interessati hanno un importante impatto economico, impedimento di accesso a fondi e finanziamenti?*	No
	4	*A causa della perdita di integrità gli interessati hanno un danno irreversibile (perdita del lavoro, impatti psicologici a lungo termine, ecc.)?*	No
PERDITA DISPONIBILITÁ	*1*	*Gli interessati possono far fronte alla perdita di disponibilità solo subendo impatti significativi e difficilmente risolvibili?*	Si
	2	*A causa della perdita di disponibilità gli interessati hanno un problema economico, una perdita di opportunità o particolari minacce?*	Si
	3	*A causa della perdita di disponibilità gli interessati hanno un importante impatto economico, impedimento di accesso a fondi e finanziamenti?*	No
	4	*A causa della perdita di disponibilità gli interessati hanno un danno irreversibile (perdita del lavoro, impatti psicologici a lungo termine, ecc.)?*	No

ANALISI DELL'ELENCO CAUSE E DELLE RISPETTIVE MISURE DI SICUREZZA

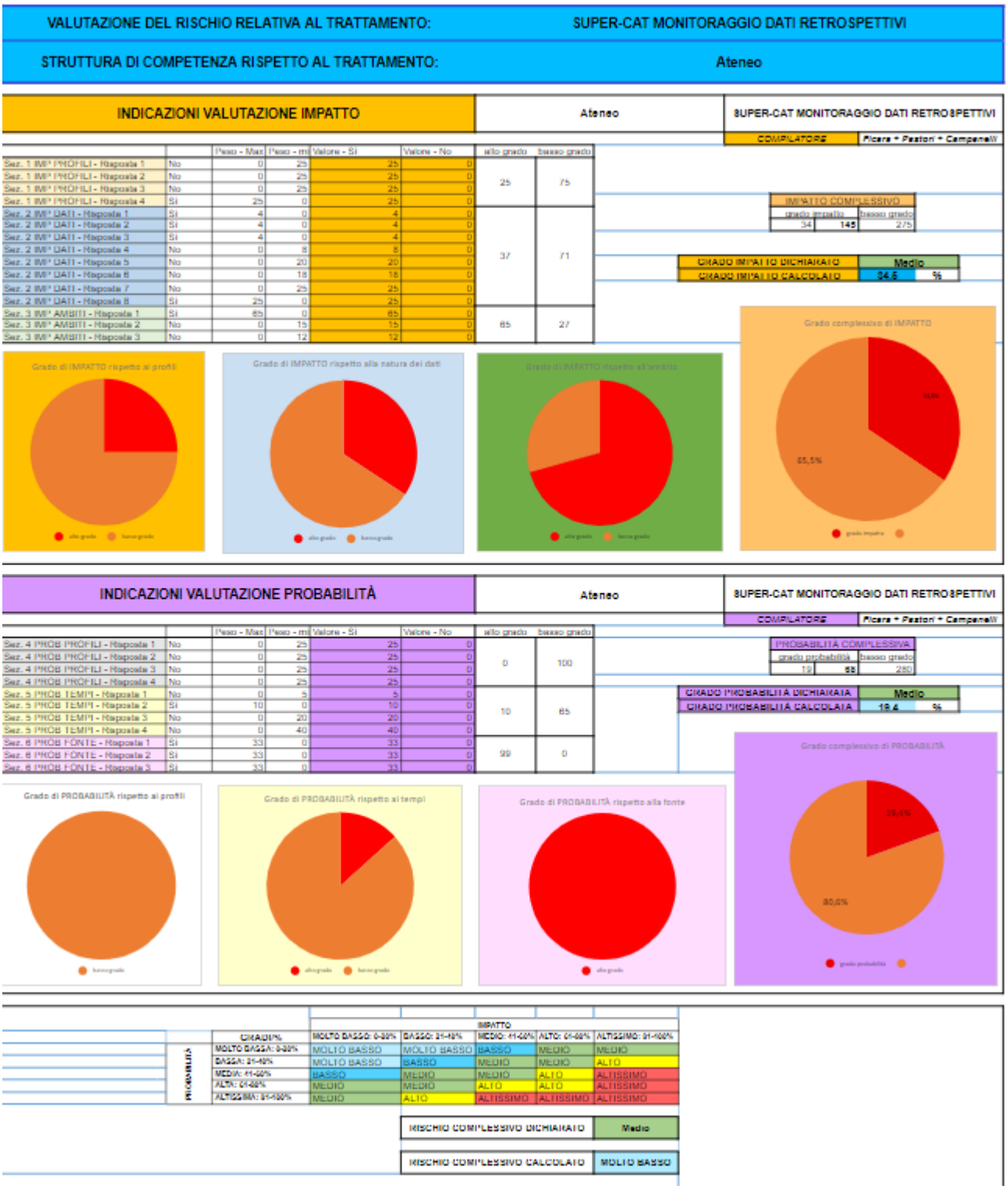
Livello di efficacia della misura	*valore*
Misura non presente o non pertinente	*[non inserire valore]*
Nullo	*1*
Base	*1,5*
Medio	*2*
Alto	*2,5*

Indicare per ogni tipo di misura di sicurezza il grado di efficacia secondo la seguente tabella:

Violazione di dati su struttura informatica e digitale: accesso abusivo, problema tecnico, errore umano, etc.	1	Controllo degli accessi logici	2
	2	Crittografia	2
	3	Archiviazione	2
	4	Lotta contro i malware	2
	5	Sicurezza dei siti web	2
	6	Aggiornamento	2
	7	Sicurezza dei canali informatici	2
	8	Controllo accessi fisici	2
	9	Gestione delle politiche di tutela della privacy	2
	10	Gestione dei rischi	2
Violazione di dati su struttura fisica e/o supposto analogico: errore umano, evento naturale distruttivo, evento distruttivo antropico, problema tecnico	1	Tracciabilità	2
	2	Archiviazione	2
	3	Manutenzione	2
	4	Controllo accessi fisici	2
	5	Gestione delle politiche di tutela della privacy	2
	6	Gestione del rischio incendio	2
	7	Gestione del rischio alluvione	2
	8	Gestione del rischio altri eventi naturali distruttivi	1,5

VALUTAZIONE DEL RISCHIO

Di seguito si riporta la valutazione del rischio calcolata.



VALUTAZIONE DEL RISCHIO RELATIVA AL TRATTAMENTO:	SUPER-CAT MONITORAGGIO DATI RETROSPETTIVI
STRUTTURA DI COMPETENZA RISPETTO AL TRATTAMENTO:	Ateneo

INDICAZIONI VALUTAZIONE IMPATTO — Ateneo — SUPER-CAT MONITORAGGIO DATI RETROSPETTIVI

COMPILATORE: Ficara + Pastori + Campanelli

		Peso - Max	Peso - min	Valore - SI	Valore - No	alto grado	basso grado
Sez. 1 IMP PROFILI - Risposta 1	No	0	25	25	0	25	75
Sez. 1 IMP PROFILI - Risposta 2	No	0	25	25	0		
Sez. 1 IMP PROFILI - Risposta 3	No	0	25	25	0		
Sez. 1 IMP PROFILI - Risposta 4	SI	25	0	25	0		
Sez. 2 IMP DATI - Risposta 1	SI	4	0	4	0	37	71
Sez. 2 IMP DATI - Risposta 2	SI	4	0	4	0		
Sez. 2 IMP DATI - Risposta 3	SI	4	0	4	0		
Sez. 2 IMP DATI - Risposta 4	No	0	8	8	0		
Sez. 2 IMP DATI - Risposta 5	No	0	20	20	0		
Sez. 2 IMP DATI - Risposta 6	No	0	18	18	0		
Sez. 2 IMP DATI - Risposta 7	No	0	25	25	0		
Sez. 2 IMP DATI - Risposta 8	SI	25	0	25	0		
Sez. 3 IMP AMBITI - Risposta 1	SI	65	0	65	0	85	27
Sez. 3 IMP AMBITI - Risposta 2	No	0	15	15	0		
Sez. 3 IMP AMBITI - Risposta 3	No	0	12	12	0		

IMPATTO COMPLESSIVO	
grado impatto	basso grado
34	145
275	

GRADO IMPATTO DICHIARATO	Medio	
GRADO IMPATTO CALCOLATO	34,5	%

INDICAZIONI VALUTAZIONE PROBABILITÀ — Ateneo — SUPER-CAT MONITORAGGIO DATI RETROSPETTIVI

COMPILATORE: Ficara + Pastori + Campanelli

		Peso - Max	Peso - min	Valore - SI	Valore - No	alto grado	basso grado
Sez. 4 PROB PROFILI - Risposta 1	No	0	25	25	0	0	100
Sez. 4 PROB PROFILI - Risposta 2	No	0	25	25	0		
Sez. 4 PROB PROFILI - Risposta 3	No	0	25	25	0		
Sez. 4 PROB PROFILI - Risposta 4	No	0	25	25	0		
Sez. 5 PROB TEMPI - Risposta 1	No	0	5	5	0	10	85
Sez. 5 PROB TEMPI - Risposta 2	SI	10	0	10	0		
Sez. 5 PROB TEMPI - Risposta 3	No	0	20	20	0		
Sez. 5 PROB TEMPI - Risposta 4	No	0	40	40	0		
Sez. 6 PROB FONTE - Risposta 1	SI	33	0	33	0	99	0
Sez. 6 PROB FONTE - Risposta 2	SI	33	0	33	0		
Sez. 6 PROB FONTE - Risposta 3	SI	33	0	33	0		

PROBABILITÀ COMPLESSIVA	
grado probabilità	basso grado
19	88
280	

GRADO PROBABILITÀ DICHIARATA	Medio	
GRADO PROBABILITÀ CALCOLATA	19,4	%

		IMPATTO				
	GRADO%	MOLTO BASSO: 0-20%	BASSO: 21-40%	MEDIO: 41-60%	ALTO: 61-80%	ALTISSIMO: 81-100%
PROBABILITÀ	MOLTO BASSA: 0-20%	MOLTO BASSO	MOLTO BASSO	BASSO	MEDIO	MEDIO
	BASSA: 21-40%	MOLTO BASSO	BASSO	MEDIO	MEDIO	ALTO
	MEDIA: 41-60%	BASSO	MEDIO	MEDIO	ALTO	ALTISSIMO
	ALTA: 61-80%	MEDIO	MEDIO	ALTO	ALTO	ALTISSIMO
	ALTISSIMA: 81-100%	MEDIO	ALTO	ALTISSIMO	ALTISSIMO	ALTISSIMO

RISCHIO COMPLESSIVO DICHIARATO	Medio
RISCHIO COMPLESSIVO CALCOLATO	MOLTO BASSO

VALUTAZIONI D'IMPATTO

Di seguito si riporta la valutazione d'impatto calcolata:

CALCOLO DPIA

CALCOLO RELATIVO AL TRATTAMENTO:	SUPER-CAT MONITORAGGIO DATI RETROSPETTIVI
STRUTTURA DI COMPETENZA:	Ateneo

VALUTAZIONE INIZIALE RISCHIO				ANALISI VALUTATIVA EFFETTI PER TIPI DI RISCHIO				RISCHIO LORDO
IMPATTO				PERDITA RISERVATEZZA	1 - RISERVATEZZA	si	1,00	98
profili	25	144,73	98		2 - RISERVATEZZA	si		
categorie	37				3 - RISERVATEZZA	no		
ambiti	65				4 - RISERVATEZZA	no		
PROBABILITA'				PERDITA INTEGRITA'	1 - INTEGRITA'	si	1,00	
profili	0	67,50			2 - INTEGRITA'	si		
tempi	10				3 - INTEGRITA'	no		
fonti	99				4 - INTEGRITA'	no		
				PERDITA DISPONIBILITA'	1 - DISPONIBILITA'	si	1,00	
					2 - DISPONIBILITA'	si		
					3 - DISPONIBILITA'	no		
					4 - DISPONIBILITA'	no		

AMBITO RISCHI/VIOLAZIONI	MISURE		RISCHIO NETTO	FATTORE EVENTI OCCORSI ULTIMI 3 ANNI		RISCHIO NETTO STORICO
	tipologia	valore		tipo	gravità	
Rischi/violazioni riguardanti dati su supporti digitali/informatici e relativi apparati	DIGITALI 1	2	97			97
	DIGITALI 2	2				
	DIGITALI 3	2				
	DIGITALI 4	2				
	DIGITALI 5	2				
	DIGITALI 6	2				
	DIGITALI 7	2				
	DIGITALI 8	2				
	DIGITALI 9	2				
	DIGITALI 10	2				
Rischi/violazioni riguardanti dati su supporti analogici/cartacei e relativi apparati	FISICI 1	2				
	FISICI 2	2				
	FISICI 3	2				
	FISICI 4	2				
	FISICI 5	2				
	FISICI 6	2				
	FISICI 7	2				
	FISICI 8	1,5				

VALUTAZIONI DEI RISULTATI E CONCLUSIONI

VALUTAZIONE SULL'IMPATTO ALLA LUCE DEL RISCHIO CALCOLATO E VALUTAZIONE COMPLESSIVA DELL'IMPATTO DEL TRATTAMENTO, TENUTO CONTO DELLE MISURE DI SICUREZZA ADOTTATE.

Considerando che lo studio clinico comporta anche il trattamento di dati sanitari, considerando l'innovatività del sistema e la delicatezza del trattamento, il **rischio iniziale** è stato **valutato** come **medio**, pertanto si è ritenuto opportuno predisporre la valutazione d'impatto (DPIA- Data Protection Impact Assessment) ex art. 35 par. 3 lett. c) GDPR.

Ai fini della valutazione d'impatto, si rileva che la valutazione iniziale del rischio, è stata sottoposta all'analisi valutativa degli effetti per tipi di rischio. Tenuto conto che il trattamento prevede il trasferimento di dati anagrafici e sanitari sulla piattaforma RedCap in forma pseudonimizzata, emerge che le misure di sicurezza adottate nell'ambito del trattamento hanno diminuito il rischio di violazioni dei dati personali e il relativo impatto per i diritti e le libertà fondamentali degli interessati.

Il **rischio calcolato** relativo al trattamento, valutato sulla scorta di parametri oggettivi predefiniti, è risultato quindi **molto basso**. Questo per il fatto che l'**impatto** calcolato del trattamento, che tiene conto delle categorie di dati trattati e dei profili del trattamento, è risultato **basso**, mentre la probabilità del rischio è risultata **molto bassa**.

Nel formulare la valutazione, si è tenuto conto della struttura organizzativa dell'ente Titolare nei seguenti termini, e tenendo conto dei seguenti aspetti.

Le infrastrutture dei data center di RedCAP si trovano all'interno dell'Unione Europea, così come i sistemi di backup e sono previste misure per garantire un accesso fisico controllato a tali data center.

Sono previste da parte di RedCAP misure di sicurezza delle reti (firewall, router ACL, network intrusion detection system), misure di sicurezza per i dati at-rest come la cifratura (algoritmo AES-256), intrusion prevention e detection system per il filtraggio di traffico non autorizzato, isolamento del database, system hardening a livello di sistema operativo, controllo accessi a livello applicativo in termini di autenticazione e autorizzazione, tramite un approccio role-based.

Per quanto riguarda l'accesso ai dati in chiaro, solo il personale sanitario coinvolto nello studio potrà poi risalire dal codice generato, al nome del paziente.

Gli eventuali rischi legati a sabotaggio o errori umani sono minimizzati in virtù della qualificazione e affidabilità degli autorizzati ed ai corsi di formazione/awareness garantiti per tutto lo staff.

Per quanto premesso, considerando che il grado complessivo di efficacia delle misure di sicurezza è dato dalla ponderazione del grado di efficacia di ogni singola misura adottata sull'infrastruttura informatica, è possibile ricondurre il grado di rischio netto ad un livello **molto basso**.

In conclusione dunque, l'impatto per i diritti e le libertà degli interessati nell'ambito del trattamento è da ritenersi **molto basso**.

Tutti i documenti istruttori sono conservati e disponibili presso l'Ufficio BICRO.

Eventuali osservazioni discostanti rispetto le risultanze dell'Ufficio di Supporto al RPD: //

Il Titolare del Trattamento

La Rettrice - Prof.ssa Giovanna Iannantuoni

Visto il RPD

Dott.ssa Emanuela Mazzotta

Il documento è firmato digitalmente ai sensi dell'art. 24 D.Lgs. 82/2005