TITOLARE DEL TRATTAMENTO	VERSIONE	NORMATIVA DI RIFERIMENTO
HUMANITAS RESEARCH HOSPITAL	Versione: **03** Data**: 12/05/2025**	Regolamento (UE) 2016/679 Decreto Legislativo 30 giugno 2003, n.196 Linee Guida 4 aprile 2017, WP 248, rev. 01

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

RICERCA OSSERVAZIONALE RETROSPETTIVA [ESTRATTO]

Disclaimer:
Il presente documento rappresenta un estratto della Valutazione d'Impatto sulla Protezione dei Dati (DPIA) relativa alla ricerca osservazionale retrospettiva. Alcune informazioni contenute nella versione originale sono state rimosse o riassunte per salvaguardare il know-how aziendale, come consentito dall'Autorità Garante per la Protezione dei Dati Personali. Le omissioni sono indicate con la dicitura "[*...omissis...*]".
Il documento completo, contenente tutte le informazioni dettagliate è messo a disposizione delle Autorità competenti su richiesta, nel rispetto degli obblighi di trasparenza previsti dalla normativa vigente.

INFORMAZIONI SUL DOCUMENTO	
Azienda titolare del trattamento:	Humanitas Mirasole S.p.A. Rozzano (MI) – Via Manzoni n. 56
Oggetto della valutazione:	Svolgimento di studi clinici di natura osservazionale retrospettiva
Data:	12/05/2025
Versione:	03
Modifica:	Revisione della versione 2 (anno 2024)
Allegati:	Nessun documento allegato
Autore del documento:	Tiziana Francolino – Referente Privacy di Gruppo
Soggetti coinvolti nella valutazione:	**Ciro Franzese –** Associate Professor of Radiation Oncology, Humanitas University, Humanitas Research Hospital IRCCS & San Pio X **Laura Bonavita** – Study Coordinator & Data Manager **Stefano De Zanet** – Study Coordinator & Data Manager **Annalisa Maroli** – Study Coordinator **Gianluca Cesare** – Responsabile dei Sistemi Informativi di Gruppo **Antonino Marsala** – Responsabile dei Sistemi Informativi della Ricerca **Luca Della Giovanna** – Chief Information Security Officer (CISO)
Soggetto preposto a sorvegliare lo svolgimento della DPIA:	Data Protection Officer di Humanitas Mirasole S.p.A.

Documenti collegati

RIFERIMENTO	SCOPO DEL DOCUMENTO
PR.RIC.01 – Protezione dei dati personali nella ricerca	Regolamenta, sotto il profilo della tutela dei dati personali, i trattamenti di dati aventi finalità di ricerca, siano essi trattamenti effettuati in studi promossi da Humanitas oppure in studi clinici promossi da altri soggetti che si avvalgono di Humanitas come centro partecipante.
Documento di Accountability – aspetti di protezione dei dati personali nel processo di ricerca clinica di Humanitas Mirasole S.p.A. (Position Paper)	Illustra gli aspetti di protezione dei dati nel processo di ricerca clinica descrivendo le motivazioni a supporto dei fondamenti di liceità del trattamento dei dati e documentando la conformità del processo e dei trattamenti che ne scaturiscono ai requisiti del Regolamento Europeo in materia di Protezione dei Dati 2016/679 (GDPR) ed alla vigente normativa collegata.
PR.CLI.06 – Organization and management of a clinical study	Fornisce una panoramica dell'organizzazione e della gestione degli studi clinici gestiti dal personale di Humanitas.

INDICE

1. PREMESSE

La **Valutazione d'Impatto sulla Protezione dei Dati** (di seguito "**DPIA**") è un processo che ogni Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone, in particolare se connesso all'impiego di nuove tecnologie.

Per effettuare la DPIA, **Humanitas Mirasole S.p.A.** segue una metodologia interna, applicata in tutte le società del Gruppo, grazie alla quale il processo è condotto secondo le indicazioni (*Guidelines on Data Protection Impact Assessment*) [1] fornite dall'ex Gruppo di lavoro "articolo 29" (Article 29 Working Party), ora European Data Protection Board (EDPB) e la valutazione dei rischi, fase centrale del processo, è effettuata seguendo un metodo formalizzato e comune a tutte le società del Gruppo descritto al paragrafo 6.1.

1.1 CONTESTO GENERALE DI APPLICAZIONE

Humanitas Mirasole S.p.A. è una società che gestisce ospedali ad alta specializzazione, operanti anche in ambito di **Ricerca clinica** e **preclinica**, sia in qualità di **IRCCS** (**Istituto Clinico Humanitas di Rozzano**), che come **strutture sanitarie non IRCCS** (**Casa di Cura San Pio X di Milano**).
Tra le missioni di **Humanitas Mirasole S.p.A.** vi è anche quella di far progredire la scienza per fare la differenza nella vita dei pazienti, orientando l'attività di ricerca sulle esigenze cliniche non soddisfatte e sfruttando conoscenze e tecnologie di alto livello per poter analizzare i meccanismi molecolari e cellulari alla base della salute e delle malattie umane.

In particolare, in Humanitas Mirasole S.p.A., tra le diverse tipologie di ricerca svolte, viene effettuata anche la **Ricerca Osservazionale Retrospettiva**, ossia la ricerca effettuata sui soli dati, tramite studi clinici che non hanno impatti diretti sulla terapia del paziente, ma sono basati solo sui dati derivanti dalla normale pratica clinica e su dati storici, retrospettivamente osservati (art. 2, par. 2, n. 4, Regolamento UE 2014/536).

[…Omissis…]

[1] cfr. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

2. NORMATIVA DI RIFERIMENTO APPLICABILE AL PROCESSO

In questa sezione sono indicate le principali fonti normative e dottrinali applicabili al processo di Valutazione di Impatto in esame:

- World Medical Association. Dichiarazione di Helsinki – Principi etici per la ricerca biomedica che coinvolge gli esseri umani. 2013; art. 32.
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR) – e in particolare l'art.35, comma 3, lett. b).
- Regolamento (UE) n. 2014/536 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE, e in particolare artt. 1, 2, 28, 29, 56, 58 e cons. 29, 76.
- Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio - e in particolare artt. 1, 2, 63, 64, 65, 66, 72 e cons. 47, 67, 89
- Decreto 30 novembre 2021 del Ministero della Salute recante le Misure volte a facilitare e sostenere la realizzazione degli studi clinici di medicinali senza scopo di lucro e degli studi osservazionali e a disciplinare la cessione di dati e risultati di sperimentazioni senza scopo di lucro a fini registrativi, ai sensi dell'art. 1, comma 1, lettera c), del decreto legislativo 14 maggio 2019, n. 52.
- Good Clinical Practice, 2.1
- EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research (adopted on 2 February 2021).
- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" – e in particolare artt. 110 e 110-bis
- Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice - n. 497 del 13 dicembre 2018
- Decreto Legislativo 5 giugno 1998, n. 204 "Disposizioni per il coordinamento, la programmazione e la valutazione della politica nazionale relativa alla ricerca scientifica e tecnologica, a norma dell'articolo 11, comma 1, lettera d), della legge 15 marzo 1997, n. 59"
- Decreto legislativo 30 dicembre 1992, n. 502 "Riordino della disciplina in materia di sanità, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421"

- Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 che istituisce il dispositivo per la ripresa e la resilienza
- Regolamento (UE) 2023/435 del Parlamento europeo e del Consiglio del 27 febbraio 2023 che modifica il regolamento (UE) 2021/241 per quanto riguarda l'inserimento di capitoli dedicati al piano REPowerEU nei piani per la ripresa e la resilienza e che modifica i regolamenti (UE) n. 1303/2013, (UE) 2021/1060 e (UE) 2021/1755, e la direttiva 2003/87/CE
- La legislazione, i regolamenti e le linee guida generali per l'attuazione del Piano Nazionale di Ripresa e Resilienza (PNRR) (rinvenibili al seguente link): https://www.italiadomani.gov.it/content/sogei-ng/it/it/home.html
- Provvedimento n. 9948285/2023 con cui il Garante per la protezione dei dati personali ha riconosciuto il programma "Horizon Europe" quale presupposto giuridico per il trattamento dei dati personali, in virtù della decisione di esecuzione della Commissione europea con cui periodicamente sono individuati i programmi e gli obiettivi di ricerca e dell'articolo 9, 2° comma lett. j) del Regolamento (UE) 2016/679
- Faq del Garante per la Protezione dei dati personali "Presupposti giuridici e principali adempimenti per il trattamento da parte degli IRCCS dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca"
- WP 248 – Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679, nello specifico cap. III, B4.
- Provvedimento del Garante per la protezione dei dati personali, n. 467, del 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[2], allegato I, pt. 6 e 10.
- Garante per la protezione dei dati personali – Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019 (Registro dei provvedimenti n. 55 del 7 marzo 2019).
- Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679
- Linee guida Linea Guida per la classificazione e conduzione degli studi osservazionali sui farmaci (det. AIFA 425/2024)

[2] v. diffusamente, 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 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979

3. VERIFICA DELLA NECESSITÀ DI DPIA

Al fine di valutare la necessità di svolgimento della **DPIA**, in conformità alla procedura di Gruppo, **Humanitas Mirasole S.p.A.** si avvale dei **nove criteri** sviluppati e descritti nella citata linea guida ratificata dal **EDPB**, **WP 248**. In generale, l'**EDPB** ritiene che maggiore sia il numero dei criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione di impatto sulla protezione dei dati personali, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare, anche allo scopo di documentarne l'efficacia e l'adeguatezza.

Come indicazione generale, la linea guida suggerisce che qualora il trattamento in esame soddisfi **almeno due** dei nove criteri individuati, esso possa ragionevolmente formare oggetto di una valutazione di impatto sulla protezione dei dati personali.

I criteri soddisfatti dal trattamento in esame sono

- Presenza di dati sensibili o aventi carattere altamente personale
- Trattamento di dati su larga scala
- Presenza di dati relativi a interessati vulnerabili
- Uso innovativo o applicazione di nuove tecnologie od organizzative

Poiché il trattamento in esame soddisfa più di due dei criteri di riferimento, Humanitas Mirasole S.p.A. ha deciso di procedere con la valutazione di impatto per tutti i tipi di ricerca clinica effettuata. Nella scelta, si è prestata particolare attenzione al fatto che lo svolgimento di attività di ricerca implica il **trattamento costante e significativo di grandi moli di dati appartenenti alle categorie particolari dei pazienti** coinvolti nei progetti di ricerca, che sono da considerarsi soggetti vulnerabili.

La scelta di Humanitas Mirasole S.p.A. di svolgere una valutazione di impatto sull'attività di ricerca complessivamente svolta, per ciascuna tipologia, e non per ogni singolo studio, è motivata e supportata dal dettato dell'articolo 35, 1 comma, del Regolamento UE 679/2016 che recita: "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*".

Più precisamente, i trattamenti di dati personali svolti nell'ambito dei singoli progetti di ricerca osservazionale retrospettiva, promossi da Humanitas Mirasole S.p.A., sono simili tra loro, così come lo sono i rischi connessi e le misure tecniche e organizzative attuate. Le attività svolte nel corso del ciclo di vita dei dati personali, come di seguito descritte (acquisizione dei dati, conservazione, pseudonimizzazione, analisi, etc.), non variano radicalmente per ogni progetto di ricerca, poiché Humanitas Mirasole S.p.A. ha ben definito la tipologia di soggetti che accedono ai dati, gli strumenti da utilizzare (es. REDCap) e le misure da attuare.

Si precisa che per la redazione della presente valutazione di impatto è stato preso in considerazione il più elevato livello di complessità in termini di trattamenti di dati personali effettuati.

4. OGGETTO DEL DOCUMENTO

Il documento di cui questo costituisce un estratto riporta l'attività di Valutazione d'Impatto **(DPIA)** condotta specificamente per lo svolgimento di studi **osservazionali retrospettivi, monocentrici** o **multicentrici** che siano, sia in qualità di **Promotore** sia in qualità di **Centro Partecipante**, e si applica sia alla ricerca "**profit**", ossia agli studi aventi finalità registrative e/o di sviluppo industriale del farmaco o del dispositivo medico, sia alla ricerca "**non profit**", ossia quegli studi che hanno come fine ultimo il miglioramento della pratica clinica, e quindi caratterizzati dall'assenza di scopo di lucro**. Oggetto del presente estratto è esclusivamente la ricerca osservazionale retrospettiva.**

5. DESCRIZIONE DEL TRATTAMENTO

5.1 TRATTAMENTO OGGETTO DI VALUTAZIONE

Il trattamento oggetto di valutazione è la **ricerca osservazionale retrospettiva** che ha come **obiettivo** quello di produrre conoscenze destinate ad avere impatto sullo stato di salute di futuri pazienti, ma non sulla vita o sul benessere diretto dei soggetti arruolati, e dall'utilizzo di un comune patrimonio di tecniche epidemiologiche e statistiche.

All'interno del presente documento vengono analizzati i **rischi** connessi al trattamento di dati personali nell'ambito delle attività di ricerca clinica sopra introdotte e sono illustrate le **misure tecniche ed organizzative** adottate dalla Società per minimizzare tali rischi.

5.2 DATI PERSONALI RACCOLTI, TRATTATI E LORO CICLO DI VITA

In ogni studio clinico, Humanitas si impegna a raccogliere unicamente i dati pertinenti e necessari per svolgere le attività di ricerca descritte nel protocollo nel pieno rispetto del principio di minimizzazione.
Considerando la dipendenza dei tipi di dati trattati dalla patologia su cui è condotto lo studio ed in generale dagli endpoints stabiliti dai ricercatori, di seguito si propone una classificazione generica dei dati personali raccolti per lo svolgimento di tali studi nelle categorie previste dal GDPR, ricostruita da un campione di studi clinici osservazionali retrospettivi condotti in Humanitas (riportando anche alcuni esempi pratici). L'elenco che segue non ha la pretesa di essere esaustivo, considerando che nuove tecnologie e continui progressi in ambito scientifico potrebbero in futuro consentire la raccolta e l'utilizzo di nuove informazioni oggi inaccessibili. Si è tuttavia ritenuto opportuno considerare la gamma più ampia possibile di dati personali generalmente trattati negli studi, soprattutto ai fini del calcolo del rischio iniziale per i diritti e le libertà dei pazienti arruolati.

DATI PERSONALI PROCESSATI NELLA RICERCA OSSERVAZIONALE	
DATI COMUNI	**Dati identificativi e anagrafici** Esempi: nome, cognome, codice fiscale, sesso, età, … **Dati di contatto** Esempi: indirizzo e-mail e numero di telefono **Dati relativi allo stile di vita** Esempi: peso, altezza, alimentazione, attività sportiva, ore di sonno, …
DATI RICONDUCIBILI A "CATEGORIE PARTICOLARI"	**Dati relativi allo stato di salute** Esempi: età di insorgenza dei sintomi, tipo di insorgenza, luogo di manifestazione dei sintomi, anamnesi famigliare, diagnosi, lo stato di fumatore, indice di massa corporea (BMI), trattamenti farmacologici ricevuti nel tempo, trattamenti farmacologici ricevuti durante il follow-up saranno raccolti retrospettivamente dalle cartelle cliniche elettroniche, dati elettrofisiologici, RMN, comorbilità …
	Dati genetici Esempi: sequenze di DNA, dati di sequenziamento del genoma, dati di scRNA-seg e metabolomica, citometria a flusso, dati quantitativi su profilerazione e migrazione…

	Campioni biologici Esempi: sangue, urine, campioni chirurgici, feci, plasma, saliva, capelli, tessuti…
	Dati relativi alla vita sessuale Esempi: orientamento sessuale, attività sessuale, storia clinica di MST (Malattie Sessualmente Trasmissibili), fertilità e riproduzione, disfunzioni sessuali…
	Dati relativi all'origine razziale o etnica Esempi: documento d'identità utilizzato per l'identificazione del paziente, dati sulla predisposizione genetica, informazioni sociodemografiche raccolte per questionari…
	Convinzioni religiose Esempi: scelte alimentari basate sulla religione, obiezione a trattamenti medici, restrizioni su farmaci…

I dati sopra elencati sono sempre trattati unicamente dai **soggetti** appositamente **autorizzati secondo le procedure interne di Humanitas**.

In particolare, sono soggetti autorizzati da Humanitas a trattare i dati personali dei pazienti arruolati:

- Medici incaricati della prestazione sanitaria (per la produzione dei source documents);
- Personale del reparto incaricato della gestione dei pazienti (per la produzione dei source documents);
- Principal Investigators (PI) dei singoli progetti di ricerca;
- Membri del team di ricerca dei PI (per la raccolta dei dati dai source documents e la loro elaborazione ed analisi);
- Data manager/Study coordinator (per la raccolta dei dati dai source documents e la loro elaborazione ed analisi)
- Personale dei sistemi informativi e/o dei fornitori dei servizi di assistenza e manutenzione ai software, per le sole attività di manutenzione dei sistemi.

Nel disegno di ogni singolo Studio il "**PI**" deve:

- **definire** - se Humanitas Mirasole S.p.A. è promotore dello Studio - oppure **verificare** - se è Centro partecipante allo Studio - la **tipologia di dati** da trattare in modo che siano minimizzati, cioè strettamente pertinenti e necessari per il perseguimento dei risultati dello Studio, e conservati per il minimo tempo necessario; e
- **personalizzare**, e poi verificare, l'apposita Sezione Privacy nel Protocollo proposta dall'Ufficio Sperimentazioni in base alla tipologia di Studio.

Dopo che i pazienti sono stati arruolati nello studio, i loro dati personali sono protetti tramite la **pseudonimizzazione** degli stessi, ossia tramite l'assegnazione a ciascun soggetto un codice univoco che non sia il suo ID paziente e che non consenta di identificarlo direttamente (per esempio, tramite nome e cognome o codice fiscale).

Al singolo **PI** o **Data Manager** è attribuita la responsabilità della conservazione della chiave di collegamento tra i dati identificativi del paziente e i suoi dati e campioni. La chiave deve essere conservata in una cartella di rete protetta e ad accesso limitato, dando l'accesso ad altri componenti del gruppo solo se strettamente necessario.
Per quanto riguarda **l'utilizzo di campioni biologici**, è compito del relativo membro del team del singolo progetto di ricerca garantire una corretta etichettatura mediante la pseudonimizzazione di cui sopra.
Successivamente il team di ricerca dovrà registrare i dati dei soggetti arruolati per lo Studio negli applicativi informatici e/o nelle **CRF** predisposte per la gestione, e archiviare i dati inerenti allo Studio.

Si precisa che tutte le procedure sopra descritte sono relative ai documenti ed ai dati della ricerca, non ai cosiddetti "documenti sorgente/source documents" che appartengono alla documentazione sanitaria del paziente e devono essere gestiti e conservati in conformità alle regole della pratica clinica (per finalità di diagnosi, terapia e assistenza).

5.3 SOGGETTI COINVOLTI E RESPONSABILITÀ

I dati trattati da **Humanitas Mirasole S.p.A.** per il perseguimento delle finalità di ricerca osservazionale sono trasmessi o eventualmente acceduti ai soggetti coinvolti a vario titolo nel trattamento, in funzione del tipo di studio, quali:

- **Autorità sanitarie competenti**: Istituzioni preposte alla valutazione e verifica della conformità dello studio per le materie di propria competenza;
- **Comitato Etico**: Ente preposto alla valutazione della eticità e scientificità dello studio;
- **Sponsor**: Promotore dello Studio nei casi di studi multicentrici;
- **Enti partner dello studio**: Centri sperimentanti o istituzioni universitarie coinvolte nel caso di studi multicentrici;
- **CRO** (Clinical Research Organization): Fornitore eventualmente incaricato di gestire e coordinare le attività di ricerca, nominato responsabile del trattamento (raramente coinvolto nella ricerca osservazionale);
- **Laboratori di analisi**: Fornitori eventualmente incaricati di svolgere analisi di campioni biologici, nominati responsabili del trattamento;
- **Provider di servizi, app o software in cloud**: Fornitori incaricati di svolgere attività di messa a disposizione e manutenzione di infrastrutture, soluzioni tecnologiche o archivistiche e nominati responsabili del trattamento.

5.4 RISORSE DI SUPPORTO AI DATI

Per poter progettare, avviare e svolgere uno studio di tipo osservazionale i soggetti coinvolti devono adottare le misure tecniche e organizzative previste dalle apposite procedure di **Humanitas Mirasole S.p.A.** Nello specifico, i dati personali degli interessati sono presenti in chiaro, per la finalità di cura (c.d. dati sorgente/source documents), negli applicativi aziendali di ogni area clinica o nel Dossier Sanitario Elettronico della struttura e vengono estratti e inseriti, manualmente con tecniche di pseudonimizzazione, all'interno dei diversi asset utilizzati da Humanitas durante la ricerca clinica,

che consistono nella piattaforma messa a disposizione da Humanitas Mirasole Spa (se Promotore) o dal Promotore dello Studio per la gestione delle eCFR.

In funzione dello studio clinico, potrebbero essere adottati o utilizzati strumenti aggiuntivi per la raccolta e l'elaborazione dei dati, come applicazioni mobili o piattaforme digitali, che tuttavia non rientrano nel campo di applicazione della presente valutazione, in quanto oggetto di una specifica analisi secondo la procedura interna di Privacy by Design, che prevede una valutazione preliminare da parte del Referente Privacy prima della presentazione del protocollo di ricerca al Comitato Etico.

6. VALUTAZIONI IN ORDINE ALLA NECESSITÀ E ALLA PROPORZIONALITÀ DEI TRATTAMENTI

6.1 SCOPO E BASE GIURIDICA DEL TRATTAMENTO

Per la tipologia di ricerca osservazionale, ai sensi del parere dell'EDPB del 02/2021 (punto 12), del dettato del D. Lgs. 196/03 e delle espressioni del Garante per la Protezione dei Dati, **Humanitas Mirasole S.p.A.** ha adottato come fondamento di liceità generale il **consenso esplicito dell'interessato**, trattandosi di ricerca svolta puramente sui dati, senza alcun intervento sull'individuo.

Nel caso della sola **ricerca osservazionale retrospettiva**, Humanitas Mirasole S.p.A. ha adottato fondamenti di liceità diversi, e precisamente:

- **La Ricerca scientifica e la qualifica di IRCCS, ai sensi dell'art, 9, comma 2, lett. j) del Regolamento UE 2016/679 e art. 110 bis, comma 4, del D. Lgs. 196**: quando il Promotore dello studio è un **IRCSS**, la normativa italiana stabilisce che il riutilizzo di dati personali non costituisce un trattamento ulteriore rispetto all'attività di assistenza sanitaria, essendo quest'ultima strumentale all'attività di ricerca, che costituisce l'attività principale degli IRCCS.
- **Il Diritto dell'Unione Europea o il diritto nazionale, ai sensi dell'art. art. 9, comma 2, lett. j), Regolamento UE 2016/679 e art. 110, comma 1, del D. Lgs. 196**: quando l'utilizzo dei dati personali per finalità di ricerca clinica è previsto nell'ambito di programmi nazionali ed europei.

Alla luce di quanto sopra esposto, Humanitas Mirasole S.p.A. ha stabilito di richiedere il **consenso** in tutti gli altri casi di studi osservazionali retrospettivi.

Quando si ravvisa l'impossibilità di informare il paziente e di raccogliere il relativo consenso, ai sensi dell'art. 110, D. Lgs. 196/2003, poiché

- **informarlo risulta impossibile (es. pazienti deceduti) o implica uno sforzo sproporzionato (es. pazienti fuori dal territorio nazionale e/o senza dati di contatto);**
- **vi sono ragioni etiche che precludono la richiesta di consenso** (informarlo rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di ricerca (es. ipotesi di malattie geneticamente trasmissibili);

è comunque possibile portare avanti lo studio, documentando i motivi di **non rintracciabilità** del paziente e l'insostituibilità dei dati dello stesso per la conduzione della ricerca (es. malattie rare).

6.2 PERIODO DI CONSERVAZIONE DEI DATI

Il **periodo di conservazione** è stabilito in ogni singolo protocollo in funzione di ogni studio e, in ogni caso, non superiore **a 25 anni**, come previsto dall'art. 58 del Regolamento (UE) 536/2014 sulla sperimentazione clinica di medicinali per uso umano. Di tale tempistica viene informato il paziente tramite apposita informativa e la sezione privacy del sito web di Humanitas dedicata alla ricerca, secondo quanto definito nella data retention policy emessa e mantenuta aggiornata da Humanitas Mirasole S.p.A.

Alla conclusione della ricerca clinica osservazionale retrospettiva, i documenti analogici utilizzati e prodotti per la specifica ricerca vengono inviati all'archivio.

6.3 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Gli interessati coinvolti nella ricerca osservazionale **retrospettiva** sono primariamente informati del trattamento tramite **informativa generale** resa al primo accesso in struttura, nello specifico, **in accettazione**.
Lo stesso documento è inoltre pubblicato sul sito web www.humanitas.it/privacy, per rendere noto il trattamento dei dati anche ai pazienti arruolati presso terzi.
Dalla stessa pagina è inoltre possibile per l'interessato richiedere l'estromissione dai progetti di ricerca in cui è stato arruolato.

Gli interessati coinvolti nella **ricerca osservazionale retrospettiva che richiede il consenso sono invece informati tramite apposito documento**, contenente una specifica e dettagliata informativa sul contenuto dello studio e sul trattamento dei dati personali, sulla base della quale possono esprimere liberamente il loro consenso.

Nella **ricerca osservazionale** retrospettiva ogni interessato riceve informazioni specifiche riguardo il trattamento dei dati (sia in termini di finalità che di modalità) e ha la facoltà, in base alla **condizione di liceità del trattamento** prevista in base al caso specifico, in qualunque momento, di:

- esercitare i propri diritti di **accesso**, **rettifica** e **limitazione del trattamento**;
- revocare il proprio consenso (**quando richiesto**) al trattamento rivolgendosi alternativamente allo Sperimentatore Principale o ai Referenti Privacy (privacy@humanitas.it) o compilando l'apposito form presente sul sito web www.humanitas.it/privacy. La revoca del consenso interrompe il trattamento ulteriore ma non attiva la necessità di cancellare i dati già raccolti e processati.
- richiedere anche la cancellazione dei propri dati dagli studi osservazionali in qualunque momento, dopo la revoca del consenso (l'esercizio del diritto di oblio implica la necessaria cancellazione dei record relativi al paziente dai database degli studi osservazionali).

Humanitas Mirasole S.p.A. ha implementato una procedura di "Gestione delle richieste di esercizio dei diritti degli interessati" (PR.PRV.02) che definisce i **ruoli** e le **responsabilità** delle Funzioni e delle Figure coinvolte nel processo di **gestione delle richieste di esercizio dei diritti degli interessati**.

6.4 FORMALIZZAZIONE DEI CONTRATTI

Gli obblighi e gli oneri posti a carico dei responsabili del trattamento sono definiti negli accordi stipulati ai sensi dell'art. 28 del Regolamento UE 2016/679, studio per studio, in funzione dei soggetti coinvolti come descritti al 5.3.

Tali accordi individuano gli ambiti e le durate dei trattamenti, le relative natura e finalità, il tipo di dati personali oggetto di trattamento, le categorie di interessati coinvolti, nonché gli obblighi ed i diritti del titolare del trattamento.

6.5 TRASFERIMENTI EXTRA SEE

In relazione alle operazioni di trattamento in esame, quando Humanitas Mirasole S.p.A. è il Promotore dello studio non è previsto il trasferimento di dati in Paesi Extra UE.
Qualora, nei casi di studi multicentrici, Humanitas Mirasole S.p.A. aderisca ad uno studio clinico promosso da terzi che prevede il trasferimento extra SEE, lo stesso è effettuato in conformità al dettato normativo degli articoli 45 e 46 del GDPR.

7. ANALISI DEI RISCHI E DELLE MISURE DI SICUREZZA

7.1 METODOLOGIA DI VALUTAZIONE DEL RISCHIO

La gestione dei rischi è effettuata a partire dalla valutazione dell'indice di **Rischio Residuo (IRR)** a valle della implementazione delle misure di protezione. La formula di calcolo del Rischio Residuo applicata è: IRR=PxG x(1-E) in un intervallo con P e G comprese tra 1 e 4 e la E calcolata tra 0 e 1.

[…Omissis…]

7.2 VALUTAZIONE DEL RISCHIO INIZIALE

[…Omissis…]

7.3 MISURE DI SICUREZZA ESISTENTI E/O PIANIFICATE

Le misure di sicurezza implementate dal Titolare del Trattamento sono descritte ed organizzate in funzione delle "risorse" messe a disposizione ed organizzate in due famiglie, valutate separatamente in termini di efficacia:

- Strumenti ed applicativi "in house"
- Strumenti ed applicativi "cloud"

e sono di seguito brevemente riassunte.

Per quanto riguarda, in particolare, gli applicativi in cloud, le misure di protezione di affidabilità, interoperabilità e sicurezza di REDCap, il software utilizzato per la gestione dei dati della ricerca, sono descritte in specifica documentazione.

Nello specifico, **le principali caratteristiche, comprese quelle infrastrutturali e di configurazione generica sono consultabili anche nella documentazione tecnica presente sul sito istituzionale** (https://projectredcap.org) e nel **repository pubblico GitHub** (https://github.com/vanderbilt-redcap). Il sistema RedCap è regolarmente licenziato e concesso in uso dal provider (Università di Vanderbilt) sia per studi non profit che profit, proprio perché utilizzato da enti di ricerca (IRCCS e Università).

I suddetti servizi sono **installati su infrastruttura cloud di un primario Cloud Service Provider**, fornitore qualificato e certificato, all'interno di data center **locati in UE** e sono gestiti interamente dal personale dei Sistemi Informativi.

Nel caso in cui Humanitas Mirasole S.p.a. non sia Promotore dello studio osservazionale ma, in qualità di Centro partecipante, si trovi nella situazione di dover utilizzare eCRF o strumenti messi a disposizione da altri soggetti, effettua una valutazione delle misure di sicurezza esistenti per gli applicativi da utilizzarsi che dovranno essere al minimo al pari di quelle descritte nella presente DPIA.

7.3.1 MISURE DI SICUREZZA STRUMENTI ED APPLICATIVI PER LA RICERCA

Sicurezza della infrastruttura tecnologica

VALUTAZIONE	CLASSIFICAZIONE
☐ **ACCETTABILE**	▪ Data center ubicati in aree che garantiscono il rispetto di requisiti minimi di sicurezza: adottata politica controlli accessi fisici, buona protezione

	da incidenti naturali (alluvione, incendio, terremoto…), Paese UE o extra UE con Decisione di Adeguatezza ▪ Adeguata politica di protezione dai malware: aggiornamenti regolari ed automatici dei software, utilizzo di buoni antivirus/antimalware, presenza di un adeguata struttura di firewall, monitoraggio attività di rete, segregazione delle reti, presenza di un SIEM adeguato alla complessità del contesto ▪ Rispetto dei "Requisiti minimi di cybersecurity" emessi dal CISO Humanitas ▪ Previsto piano per la gestione degli incidenti e del disaster recovery

Controllo degli accessi logici

VALUTAZIONE	CLASSIFICAZIONE
☐ **ACCETTABILE**	▪ Applicata politica password sicura: lunghezza di almeno 12 caratteri, case sensitive, con caratteri speciali, scadenza frequente, definita politica di ripristino (es. uso del numero di telefono, indirizzo email alternativo…), blocco in caso di multipli tentativi di accesso ▪ Definita procedura di assegnazione e revoca utenze ▪ Applicato il principio del minimo privilegio: accessi privilegiati in base alla funzione svolta, utenze univoche e nominali separate dalle utenze di operatore ordinario ▪ Processo di autenticazione a più fattori (MFA) (almeno su asset critici, accessi privilegiati e applicazioni da remoto) ▪ Previsto il monitoraggio degli accessi (analisi log) ▪ Garantiti adeguati livelli di sicurezza per collegamento da remoto (VPN) ▪ Prevista formazione utenti (tramite procedure e/o corsi di formazione) ▪ Buoni controlli per Amministratori di Sistema: correttamente individuati e nominati, segregazione dei compiti

Conservazione

VALUTAZIONE	CLASSIFICAZIONE
☐ **MIGLIORABILE**	▪ Applicate tecniche di crittografia ai database o agli storage ▪ Applicate tecniche di pseudonimizzazione ▪ I dati sono correttamente conservati: possibilità di cancellazione dei dati secondo regole di cancellazione sicura, impossibilità di modifica diretta dei dati inseriti nel database

Archiviazione

VALUTAZIONE	CLASSIFICAZIONE

☐ **MIGLIORABILE**	▪ I dati sono conservati per il solo tempo necessario al raggiungimento delle finalità (indicato con chiarezza il periodo di conservazione e/o la normativa che lo determina)
	▪ Metodo di archiviazione impostato:
	  ○ Definiti i criteri di archiviazione
	  ○ Effettuata una classificazione dei dati

Backup

VALUTAZIONE	CLASSIFICAZIONE

☐ **ACCETTABILE**	▪ Adeguate politiche di backup: retention adeguata, supporti cifrati, spazi segregati fisicamente dai sistemi di produzione (macchine diverse o building), spazi segregati logicamente dal sistema di produzione (istanze diverse), backup automatizzati, periodici test di ripristino ▪ Presenza (e verifica dell'efficacia) di soluzioni di disaster recovery

Gestione delle postazioni

VALUTAZIONE	CLASSIFICAZIONE
☐ **ACCETTABILE**	▪ Redatto un regolamento/linee guida per una corretta gestione delle postazioni: gestione dei documenti, gestione password, best practises per la navigazione in internet, politiche BYOD, installazione nuovi software, gestione posta elettronica, politiche lavoro da remoto, segnalazione incidenti… ▪ Effettuata configurazioni iniziale sicura dei dispositivi aziendali ▪ Prevista la formazione del personale circa la gestione delle postazioni

Canali di comunicazione e trasferimenti

VALUTAZIONE	CLASSIFICAZIONE
☐ **ACCETTABILE**	▪ Sistema di trasmissione con adeguati requisiti di sicurezza: canale crittografato, accesso limitato ai dati, possibile cancellazione dei dati una volta trasmessi… ▪ In caso di trasferimenti: o Soddisfatte le garanzie previste dal GDPR per i trasferimenti extra SEE (Decisione di Adeguatezza, BCR, SCC…) o Non previsti ulteriori trasferimenti successivi da parte del destinatario dei dati o Cifratura dei dati in viaggio

Tracciabilità

VALUTAZIONE	CLASSIFICAZIONE
☐ **ACCETTABILE**	▪ Politica di raccolta dei log adeguata: chiaramente definite l'estensione e gli obiettivi di registrazione (monitoraggio della sicurezza, la risoluzione dei problemi, la conformità normativa, ecc.), raccolta dei soli log necessari alle finalità, separazione dei log, crittografia, controllo accessi (accesso ai log garantito a poche persone), backup regolare, Politica di conservazione dei log adeguata (periodo di conservazione conforme alla normativa, adeguato rispetto alle finalità…) ▪ Documentazione delle politiche adottate, delle scelte in termini di necessità ed estensione, adeguata informativa agli utenti ▪

Gestione delle vulnerabilità

☐ **ACCETTABILE**	▪ Implementata una politica per la gestione delle vulnerabilità, compresa la gestione delle patch critiche raccomandate dalla casa produttrice del software ▪ Previsto il regolare monitoraggio per la rilevazione di attività sospette ▪ Effettuazione di valutazioni periodiche per l'individuazione di vulnerabilità (vulnerability assessment) ▪ Effettuazione di test periodici di simulazione di attacchi ed intrusioni (pen test)

Gestione degli incidenti di sicurezza e delle violazioni dei dati personali

VALUTAZIONE	CLASSIFICAZIONE
☐ **ACCETTABILE**	▪ Adottata e documentata la politica per la gestione degli incidenti (e dei near misses) di sicurezza (rilevazione, gestione, comunicazione), integrata con la gestione del data breach ▪ Effettuata attività di formazione per la gestione degli incidenti ▪ Individuate all'interno dell'azienda le figure responsabili per la gestione degli incidenti ▪ Presenza di piani di business continuity

Contratti con i responsabili del trattamento

VALUTAZIONE	CLASSIFICAZIONE
☐ **ACCETTABILE**	▪ Sono correttamente individuati i responsabili del trattamento ▪ Tutti i responsabili sono vincolati contrattualmente ai sensi dell'articolo 28 del Regolamento UE 2016/679 ▪ I responsabili individuati presentano sono dotati di certificazioni che garantiscono l'adeguatezza delle misure di sicurezza e dei servizi svolti

7.4 ESITO DELLA VALUTAZIONE DEL RISCHIO RESIDUO

Applicato il metodo di valutazione dei rischi adottato dall'Organizzazione, si ottiene per il trattamento in esame il seguente indice di rischio residuo "IRR", tenendo conto delle misure di sicurezza raccomandate per le due tipologie di trattamenti ed applicativi (in house o esternalizzati).
Date le misure di sicurezza già implementate (e potenziabili con le raccomandazioni per il miglioramento) il rischio residuo ottenuto per tutti i parametri RID risulta basso per la ricerca osservazionale retrospettiva.

Le **soluzioni adottate** per il rispetto dei principi fondamentali posti alla base della protezione dei dati e per far fronte ai rischi per le libertà e i diritti degli interessati **sono quindi considerate complessivamente accettabili**. L'implementazione progressiva di ulteriori misure tecniche ed organizzative, così come lo svolgimento di successivi controlli e l'aggiornamento della DPIA rappresentano, in ogni caso, attività necessarie al fine di garantire un'adeguata e costante protezione dei dati.

Di seguito si riportano nuovamente i criteri di gestione del rischio descritti nel dettaglio al paragrafo 7.1 al solo scopo di facilitare la lettura dei risultati della analisi svolta.

Tab. C	CLASSIFICAZIONE DEL RISCHIO				
		LIVELLI DI GRAVITÀ DEL DANNO QUALITATIVI (G)			
		trascurabile	limitato	importante	massimo
		1	2	3	4
LIVELLI DI PROBABILITÀ SEMI-QUANTITATIVI (P)	estremamente improbabile 1	**1**	**2**	**3**	**4**
	bassa probabilità 2	**2**	**4**	**6**	**8**
	moderata probabilità 3	**3**	**6**	**9**	**12**
	alta probabilità 4	**4**	**8**	**12**	**16**

- I **valori x<4** risultano essere **rischi trascurabili**
- I **valori 4≤x<6** sono considerati **rischi bassi**
- I **valori 6≤x<9** sono considerati **rischi medi**
- I **valori x>=9** sono considerati rischi alti, quindi **non accettabili**

7.4.1 ESITO DELLA VALUTAZIONE DEL RISCHIO SULLA RICERCA RETROSPETTIVA

STUDI OSSERVAZIONALI RETROSPETTIVI						
Violazione di	**Possibili impatti sui diritti e le libertà delle persone**	**G**	**P**	**R**	**E**	**IRR**
riservatezza	Compromissione della confidenzialità e della riservatezza relative a dati personali comuni e particolari dell'interessato, con particolare attenzione alle informazioni di natura genetica. […omissis…] **DIscriminazione, esclusione sociale, danno di immagine, disturbo psicologico**	[…omissis…]	[…omissis…]	[…omissis…]	[…omissis…]	4,11
integrità	Compromissione dell'integrità dei dati personali comuni e particolari dell'interessato, con particolare attenzione alle informazioni di natura genetica. […omissis…] **Ritardi, difficoltà di contatto, sfiducia**	[…omissis…]	[…omissis…]	[…omissis…]	[…omissis…]	0,50
disponibilità	Indisponibilità di dati personali comuni e particolari dell'interessato, con particolare attenzione alle informazioni di natura genetica ed al materiale biologico. […omissis…] **Ritardi, difficoltà di contatto, sfiducia**	[…omissis…]	[…omissis…]	[…omissis…]	[…omissis…]	0,48

8. PARERE DEL DPO

La presente valutazione di impatto è redatta in conformità ai requisiti dell'articolo 35 del GDPR ed alla linea guida WP248 del European Data Protection Board e ne contiene tutti gli elementi essenziali:

- sono descritte la natura, l'ambito di applicazione, il contesto e le finalità del trattamento;
- sono evidenziati le categorie di dati personali, i destinatari e il periodo di conservazione dei dati personali;
- è fornita una descrizione sintetica delle attività del trattamento e del ciclo di vita dei dati, ulteriormente ben documentati nelle procedure e nei documenti collegati ed elencati nel documento;
- sono individuati i principali sistemi attraverso i quali si effettuano i trattamenti e le regole di sicurezza minime per l'utilizzo di applicazioni studio-specifiche;
- sono valutate necessità e proporzionalità dei dati personali rispetto alle finalità della ricerca, anche con riferimento ai rispettivi protocolli;
- sono determinate le misure previste per garantire il rispetto del GDPR (principi base del trattamento, modalità di esercizio dei diritti degli interessati, rapporti con i responsabili del trattamento, assenza di trasferimenti extra SEE di default e relative misure di garanzia qualora necessario il trasferimento);
- i rischi per i diritti e le libertà degli interessati sono individuati, valutati e gestiti;
- l'origine, la natura, la particolarità e la gravità dei rischi vengono determinate dalla prospettiva degli interessati;
- sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
- sono stimate la probabilità e la gravità;
- sono determinate le misure previste per gestire tali rischi.

Il personale dei Sistemi Informativi (generali e della ricerca) è stato coinvolto per la raccolta e valutazione delle misure di sicurezza. Parimenti, un nucleo di PI e Data Manager è stato coinvolto per raccogliere degli studi campione, ricostruire il ciclo di vita dei dati e valutare il rischio iniziale per i diritti e le libertà delle persone.
Il DPO è stato consultato e coinvolto nel processo.

Non sono state raccolte le opinioni degli interessati perché la materia è tecnica, gli interessati sono soggetti vulnerabili, difficilmente raggiungibili e non specificamente esperti né di sicurezza delle informazioni né di etica (ma sono sempre puntualmente informati tramite le apposite pagine web messe a disposizione dall'organizzazione ed una sintesi di questo documento è pubblicata sul web).
Per quanto concerne le misure di protezione, il DPO rileva l'utilità di applicare i miglioramenti indicati per la promozione dell'uso estensivo di RedCap per lo svolgimento di tutte le attività di ricerca osservazionale.

Il DPO di Humanitas Mirasole S.p.A.

9. VALIDAZIONE DELLA DPIA DA PARTE DEL TITOLARE DEL TRATTAMENTO

Il legale rappresentante del titolare Humanitas Mirasole S.p.A. convalida la DPIA alla luce dell'analisi effettuata.

Le soluzioni adottate per il rispetto dei principi fondamentali posti alla base della protezione dei dati e per far fronte ai rischi per le libertà e i diritti degli interessati, al netto degli scenari migliorativi rilevati, sono state considerate complessivamente accettabili. L'implementazione progressiva di ulteriori misure tecniche ed organizzative, così come lo svolgimento di successivi controlli e l'aggiornamento della DPIA rappresentano, in ogni caso, attività necessarie al fine di garantire un'adeguata e costante protezione dei dati.

Humanitas Mirasole S.p.A.
Il legale rappresentante