VALUTAZIONE D'IMPATTO PRIVACY (DPIA)

CONTESTO DEL TRATTAMENTO OGGETTO DI VALUTAZIONE D'IMPATTO

Visione d'insieme

Presentazione del(dei) trattamento(i) considerato(i)

Descrizione del trattamento	Studio osservazionale retrospettivo multicentrico no profit dal titolo: "Tools guidati dall'intelligenza artificiale per le malattie aortiche e le comorbidità cardiovascolari – TIA-MAC". Progetto RAISE Spoke 2, WP 4 Task 4.3 "AI-driven tools for primary aortic diseases and cardiovascular comorbidities". Lo studio è promosso dall'Università degli studi di Genova - DISC - Dipartimento di Scienze Chirurgiche e Diagnostiche Integrate. Ogni anno le malattie cardiovascolari causano oltre 220.000 decessi, pari al 44% dei decessi totali. La maggior parte delle malattie cardiovascolari, incluse quelle aortiche come (aneurismi e dissezioni), possono rimanere asintomatiche fino alla rottura o alla manifestazione acuta con mortalità associata fino al 50%. Nella routine clinica, queste patologie potrebbero essere evidenziate in indagini diagnostiche effettuate per altri motivi; in questi casi sarebbe opportuno avviare un opportuno piano di sorveglianza quando queste patologie vengono diagnosticate ad uno stato iniziale. Tra i metodi di Artificial Intelligence (AI), il deep learning (DL) sta emergendo come una potente classe di algoritmi basati su reti neurali artificiali. Alla luce di tutto ciò, ne deriva l'importanza di utilizzare algoritmi di DL per l'identificazione delle strutture anatomiche di interesse e la previsione della loro possibile evoluzione, consentendo l'implementazione della prevenzione, la riduzione del rischio e l'ottimizzazione delle risorse disponibili. Valutazione retrospettiva di immagini diagnostiche pre-operatorie e di follow-up riferite al distretto aortico eseguite nell'intervallo temporale Ottobre 2014 – Settembre 2024. Il progetto sarà basato sull'analisi delle immagini diagnostiche per la diagnosi, lo screening, ed il follow-up della patologie aortiche. I dati raccolti saranno utilizzati per la stratificazione del rischio

	cardiovascolare e predizione di complicanze post-operatorie dopo il trattamento endovascolare aortico. I dati diagnostici dei pazienti arruolati retrospettivamente (gruppo di controllo e gruppo affetto da patologie vascolari aortiche) verranno utilizzati per l'addestramento delle reti neurali ed integrati con la storia clinica dei soggetti, per caratterizzare un profilo di rischio paziente-specifico. Inoltre, partendo dall'identificazione della patologia, una pipeline di valutazione integrata consentirà di prevedere l'evoluzione della malattia per il singolo paziente, al fine di stabilire una stratificazione personalizzata degli intervalli di sorveglianza dopo il trattamento ottimizzando il follow-up. In sintesi l'obiettivo è di analizzare retrospettivamente immagini diagnostiche dei pazienti partecipanti per l'addestramento delle reti neurali a fine di diagnosi, screening, ed follow-up della patologie aortiche. Verranno utilizzati dati della storia clinica dei pazienti per caratterizzare un profilo di rischio paziente-specifico. Lo studio prevede di arruolare tutti soggetti afferiti tra Ottobre 2014 e Settembre 2024 presso le UO di Radiologia dell'IRCCS Ospedale Policlinico San Martino di Genova e UO di Radiologia dell'E.O. Ospedali Galliera di Genova. I Pazienti arruolati, esclusivamente adulti, verranno suddivisi in due gruppi: Gruppo A soggetti affetti da patologia aortica (800 pazienti), Gruppo B pazienti non affetti da patologia aortica (1200 pazienti). Le immagini diagnostiche e i dati clinici saranno raccolti in forma pseudonimizzata e utilizzati per l'arruolamento delle reti neurali e la successiva analisi geometrica, ove applicabile. L'intero set di 2000 pazienti sarà suddiviso in un set di addestramento (75% dei dati) utilizzato per addestrare le reti, un set di convalida (10% dei dati) utilizzato per prevenire l'overfitting e mettere a punto il modello e un set di test (15 % dei dati) per valutare le prestazioni del modello. Verrà sviluppata una pipeline basata sull'apprendimento automatico per individuare e segmentare la regione vascolare di interesse (aorta e suoi vasi collaterali principali) dalle immagini Angio-TC. Una volta ottenute le segmentazioni automatiche per tutti i casi del dataset verranno estratte le informazioni quantitative dell'analisi geometrica dal lume aortico e della trombosi, qualora presente, per mezzo di librerie dedicate Python. I dati clinici e i dati ottenuti dell'analisi geometrica verranno utilizzati per addestrare una nuova rete neurale al fine di creare un modello predittivo che stratifichi il rischio cardiovascolare dei soggetti.

Titolare del trattamento	- Dipartimento di Scienze Chirurgiche Diagnostiche e Integrate, Università degli Studi di Genova (Promotore) - E.O. Ospedale Galliera Mura delle Cappuccine 14 16128 Genova (centro partecipante)
Referenti interni/strutture interne coinvolti	Dirigente Medico Dott. Francesco Paparo presso S.C. Radiodiagnostica dell'E.O. Ospedali Galliera (centro partecipante).
Eventuali responsabili esterni	n/a
Eventuali sub-responsabili (specificare di quale responsabile)	n/a
Eventuali contitolari del trattamento	n/a

STUDIO DEI PRINCIPI FONDAMENTALI

Valutazione delle misure poste a garanzia della proporzionalità e necessarietà del trattamento

Precisare la finalità perseguita e indicare gli elementi che rendono legittimo perseguirla

Finalità	Legittimità
Ricerca scientifica	Il trattamento dei dati personali necessario per la realizzazione dello studio ha come base giuridica principale il consenso ai sensi degli artt. 6 par. 1 lett. a) e 9 par. 2 lett. a) del GDPR. Ai sensi dell'articolo 110 del Codice Privacy e delle Regole Deontologiche di maggio 2024, una parte dei dati utilizzati saranno raccolti senza il consenso degli interessati per le ragioni più oltre precisate. Lo studio in questione è stato oggetto di espressa approvazione, anche con riferimento a questo aspetto, da parte del Comitato Etico della Liguria nella seduta del 10/02/2025 codice identificativo N. CET - Liguria 439/2024 – ID 14137. Il documenti è visibile e disponibile presso i titolari del trattamento ed il comitato etico di riferimento.

Dati, destinatari, pertinenza, minimizzazione e durata della conservazione

Descrizione delle tipologie di dati oggetto di trattamento *(C= comuni / S= categorie particolari / G= giudiziari)*, fonte di provenienza ed eventuali destinatari esterni, applicazione del principio della "minimizzazione" dei dati trattati (i dati devono essere adeguati, pertinenti, non eccedenti rispetto alle finalità perseguite), durata della conservazione prevista

	Dettaglio dei dati trattati	Tipo di dati (C/S/G)	Fonte di provenienza dei dati	Eventuali destinatari esterni	Giustificazione della pertinenza dei dati rispetto alle finalità	Misure di minimizzazione	Durata della conservazione	Giustificazione della durata della conservazione	Modalità di distruzione al termine della conservazione
1	Anagrafici	C	Raccolti direttamente dal partecipante o dall'eventuale rappresentante legale o dalla cartella clinica	Al promotore solo variabili non direttamente identificative	Variabili imprescindibili per la conduzione dello studio: es. età, sesso, luogo di nascita	Nei dati anagrafici di contatto si richiede l'indicazione della sola modalità di contatto preferita dal partecipante, allo scopo di minimizzare le informazioni raccolte a quelle strettamente necessarie.	I dati saranno conservati per circa 10 anni, tempo necessario alla raccolta ed elaborazione dei dati.	I termini indicati rappresentano quelli strettamente necessari per la raccolta dati, la pulizia del data base e l'analisi statistica, come indicato nel protocollo di studio.	Il materiale cartaceo sarà distrutto e quello informatico cancellato da parte degli operatori coinvolti nello svolgimento dello studio. Le procedure di distruzione saranno tracciate e rese disponibili all'interessato.
2	Clinici	S	Raccolti dalle cartelle cliniche e dai referti.	Al promotore solo variabili non direttamente identificative	Variabili imprescindibili per la conduzione dello studio.	Si raccolgono esclusivamente i dati previsti dal protocollo ed inseriti nelle Case Report Form.	Come sopra	Come sopra	Come sopra

Chiarire come si dimostra che i dati oggetto di trattamento sono sempre esatti e aggiornati

Misure per garantire la qualità dei dati
I dati anagrafici e clinici vengono raccolti retrospettivamente dalla cartella del paziente, dai referti di indagini strumentali e clinici. La gestione del database è sotto la responsabilità del promotore che agisce come titolare del trattamento per quanto riguarda la gestione dei dati nell'ambito dello studio stesso, fornendo CRFs, istruzioni operative, autorizzazioni all'inserimento dati, controlli di qualità, gestione e pulizia dei dati, analisi statistiche complete, archiviazione e supporto amministrativo durante tutto il corso dello studio. È responsabilità dello sperimentatore garantire che le Case Report Form (CRF) siano complete e corrispondano ai dati originali, è responsabilità del promotore effettuare controlli di accuratezza e verifica della qualità del dato.

Base giuridica del trattamento

Barrare la/le voce/i che interessa/interessano per i dati comuni.

	Per i DATI "COMUNI" (es. anagrafiche, numero di telefono, indirizzo e-mail)
☒	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità
☒	Si applica l'articolo 110 del Codice Privacy per i casi in cui non sia stato possibile raccogliere il consenso degli interessati.
☐	il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso
☐	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento PRECISARE LA FONTE NORMATIVA DELL'OBBLIGO:
☐	il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica
☐	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento PRECISARE QUALE:

Barrare la/le voce/i che interessa/interessano per le categorie particolari di dati.

	Per le CATEGORIE PARTICOLARI DI DATI (es. stato di salute, orientamento sessuale, dati genetici, orientamento religioso, ecc.)
☒	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche
☒	Si applica l'articolo 110 del Codice Privacy per i casi in cui non sia stato possibile raccogliere il consenso degli interessati.
☐	il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo
☐	il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso
☐	il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato
☐	il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali
☐	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato PRECISARE QUALE:
☐	il trattamento è 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 sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità
☐	il trattamento è 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, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale
☐	il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Valutazione delle misure a protezione dei diritti personali degli interessati

Determinazione e descrizione delle misure adottate per fornire l'informativa agli interessati di cui agli artt. 13 e 14 GDPR.

Misure per garantire il diritto all'informativa	Giustificazione dell'eventuale esenzione
I pazienti potenzialmente eleggibili che effettuano controlli presso l'Ente saranno preventivamente informati delle caratteristiche dello studio, dei suoi diritti, dell'assenza di rischi e anche dell'assenza di benefici attraverso due informative con consenso informato. La prima informativa con consenso è studio specifica e riporterà le caratteristiche e le finalità dello studio, il Comitato Etico che ha valutato lo studio, i contatti dei ricercatori, i diritti e le tutele del paziente in accordo alle Norme di Buona Pratica Clinica e alla normativa vigente sugli studi clinici. La seconda informativa con consenso riguarda il trattamento dei dati personali e descrive tutti i diritti del paziente in ambito di privacy, il titolare del trattamento dei dati con i recapiti anche del DPO, le modalità per esercitare i propri diritti, la tipologia di dati raccolti e la durata della loro conservazione oltre che informazioni generali sulla privacy. I pazienti eleggibili, se decidono di partecipare allo studio, dovranno firmare entrambi i consensi proposti (studio e privacy), avranno il tempo di porre tutte le domande che riterranno opportuno fare e per decidere se partecipare alla ricerca, saranno inoltre informati del loro diritto di ritirare i consensi in qualsiasi momento. Ove applicabile le informative saranno proposte al legale rappresentate, qualora ai pazienti arruolati decadano le motivazioni per il tutoraggio, l'informativa sarà somministrata al paziente che potrà decidere in autonomia se continuare lo studio oppure se uscire dalla ricerca. Tutte le informative con consenso proposte ai pazienti partecipanti alla ricerca sono state approvata dal Comitato Etico Territoriale della Liguria. Per i pazienti non contattabili o deceduti si veda il paragrafo "giustificazione dell'eventuale esenzione".	In caso di incapacità del partecipante a ricevere le informative le stesse saranno somministrate al legale rappresentante. Qualora gli interessati in questione siano soggetti deceduti oppure che non possono essere contattati per: -motivi etici: quando l'interessato ignora la propria condizione e rendere l'informativa privacy comporterebbe la rivelazione di notizie in merito allo conduzione dello studio suscettibili di arrecare un danno materiale o psicologico all'interessato stesso; - motivi organizzativi: quando non utilizzare i dati relativi ai soggetti non contattabili produrrebbe conseguenze significative sulla qualità dei risultati della ricerca o quando contattare gli interessati implicherebbe uno sforzo sproporzionato in considerazione dell'elevata numerosità del campione per lo studio.lil Promotore si impegna ad adottare misure di sicurezza appropriate ai rischi connessi alla ricerca al fine di tutelare i diritti, le libertà e gli interessi legittimi dell'interessato, nel pieno rispetto del principio di accountability; acquisire il parere favorevole del Comitato etico competente a livello territoriale sul progetto di ricerca; spiegare e documentare nel progetto di ricerca le ragioni (etiche o organizzative) per le quali l'acquisizione del consenso dell'interessato risulta impossibile o implica uno sforzo sproporzionato o rischia di compromettere il conseguimento delle finalità della ricerca; svolgere e pubblicare la valutazione di impatto ai sensi dell'articolo 35 del GDPR, dandone comunicazione al Garante privacy. A maggior tutela degli interessati, anche il Centro di sperimentazione (E.O. Ospedali Galliera) svolge, sulla base delle informazioni messe a sua disposizione dal Promotore, la presente valutazione d'impatto.

Determinazione e descrizione delle misure per raccogliere il consenso (se applicabile).

Misure per la raccolta del consenso	Giustificazione dell'eventuale impossibilità della loro messa in opera
Fatta salva la componente retrospettiva senza consenso sopra dettagliata, al paziente seguito presso l'Ente sarà proposta l'informativa con consenso allo studio e in relazione al trattamento dei suoi dati personali nel corso di un colloquio esplicativo durante il quale il paziente avrà tempo di fare tutte le domande che ritiene opportune e riflettere se aderire o meno alla ricerca. Solo alla fine di un esauriente colloquio gli saranno somministrati i due consensi. Il paziente potrà anche portarsi a casa le informative per discuterne con persone di sua fiducia dopodiché, qualora decidesse di partecipare alla ricerca, dovrà firmare entrambi consensi (quello alla ricerca e quello al connesso trattamento dei suoi dati anche appartenenti a categorie particolari). Una copia delle informative e dei consensi informati resteranno al paziente mentre gli originali rimarranno nella documentazione locale dello studio.	Si vedano le motivazioni espresse sopra.

Determinazione e descrizione delle misure per l'esercizio dei diritti di cui al GDPR (ARTT. 15 E SS.)

	Indicare i diritti applicabili al trattamento in questione
☒	ACCESSO (art. 15)
☒	RETTIFICA (art. 16)
☒	CANCELLAZIONE/OBLIO (art. 17)
☒	LIMITAZIONE DEL TRATTAMENTO (art. 18)
☒	NOTIFICA IN CASO DI RETTIFICA/CANCELLAZIONE E/O LIMITAZIONE (art. 19)
☒	PORTABILITÀ (art. 20)
☒	OPPOSIZIONE (art. 21)
☒	NON ESSERE SOTTOPOSTO A UNA DECISIONE BASATA UNICAMENTE SUL TRATTAMENTO AUTOMATIZZATO, COMPRESA LA PROFILAZIONE (art. 22)

Se rispetto al trattamento in questione non possono essere esercitati uno o più diritti, motivarlo:

Giustificazione
n/a

Gestione del riscontro agli interessati che esercitano un diritto.

Modalità prevista per la risposta agli interessati che esercitano un diritto:
Il riscontro viene fornito direttamente dal Responsabile Protezione Dati (DPO) dell'Ente.

Trasferimento extra-UE dei dati

Determinazione e descrizione delle misure per l'eventuale trasferimento dei dati al di fuori dell'Unione Europea

Tipologia di dati oggetto di trasferimento	Motivazione del trasferimento	Soggetto destinatario	Paese destinatario	Legittimante del trasferimento (decisione di adeguatezza, clausole contrattuali tipo, regole vincolanti di impresa, altre misure di cui all'art. 49 GDPR fra cui consenso, ecc.)
n/a				

MISURE DI SICUREZZA

Valutazione delle misure di sicurezza

Descrizione e valutazione delle misure che contribuiscono a contenere i rischi legati alla sicurezza dei dati (art. 32) circa l'intera attività di trattamento:

Misure specifiche applicate sui dati trattati	Modalità operative
Cifratura	I dati saranno soggetti a una forma di crittografia consistente nel criptare i dati per renderli incomprensibili a prima vista.
Pseudonimizzazione	Prevista dal protocollo, al paziente sarà assegnato un codice univoco che sarà utilizzato in ogni scheda di raccolta dati. Solo presso l'Ente sarà possibile collegare il codice allo stesso paziente. Questa informazione sarà distrutta a fine studio.
Protezione dei dati in rapporto al sistema utilizzato	Solo agli sperimentatori autorizzati dal responsabile dello studio sarà possibile accedere ai dati con modalità di trattamento differenti a seconda del ruolo nello studio. Le CRFs avranno un accesso controllato dalle procedure previste dal sistema aziendale e dal software utilizzato.
Controllo degli accessi logici	Credenziali personali attribuite dal sistema aziendale.
Tracciabilità degli accessi	Il software utilizzato per la raccolta dati permette di tracciare gli accessi, gli inserimenti e le modifiche ai dati. Specifiche istruzioni operative sono previste dal software e dal protocollo di studio.
Controllo di integrità	Specifiche istruzioni operative sono adottate dal sistema informatico e dall'organizzazione dello studio per mantenere l'integrità dei dati.
Modalità di archiviazione	Il materiale informatico sarà conservato su server locali gestito secondo le norme del GDPR. Ogni sistema informatico utilizzato nell'ambito dello studio prevede backup giornalieri secondo le procedure previste dalle organizzazioni aziendali ospedaliere. Il materiale cartaceo sarà archiviato in locali appositi con accesso di personale controllato e autorizzato e con sistemi di sicurezza ambientali forniti dalle strutture ospedaliere (es. antincendio).
Sicurezza dei documenti cartacei	Locali accessibili solo agli sperimentatori.
Istruzioni persone autorizzate	Il personale delegato per le attività dello studio viene istruito sulla corretta gestione dei dati del paziente
Politiche di trasmissione dei dati	Per questo studio il promotore fornirà ai Centri partecipanti delle istruzioni in ordine alla trasmissione sicura di dati al promotore: trasmissione di file xls con dati pseudonimizzati mediante posta elettronica e file protetto da password. La password non sarà inviata allo stesso indirizzo di posta elettronica.

Policy di gestione data breach	Il promotore ha adottato una procedura di gestione delle violazioni dei dati personali in cui sono definite le modalità operative da seguire in casi di incidente. Tale procedura disciplina anche le violazioni esterne al promotore. Anche l'E.O. Ospedali Galliera si è dotato di una propria procedura che disciplina la gestione delle eventuali violazioni dei dati personali dallo stesso trattati.

Nel caso di trattamenti svolti per mezzo di uno specifico software

Denominazione software	REDCap (Research Electronic Data Capture) – Il Centro non utilizza altri software né sistemi di intelligenza artificiale per elaborare i dati prima del trasferimento al Promotore.
Fornitore del software	Vanderbilt University - Il data base sarà predisposto dal promotore

Descrizione sintetica attività gestita	L'accesso alla piattaforma RedCap è gestito direttamente da UniGe – DISC, che si occupa della creazione degli account e dell'assegnazione dei privilegi (solo visione, modifica, download, ecc.). Ogni centro partecipante a uno studio registrato sulla piattaforma dovrà fornire il nome, il cognome, e la mail della persona incaricata del data entry. Questa persona sarà abilitata dalla sezione di Biostatistica e riceverà un'e-mail automatica dal sistema RedCap per effettuare il primo accesso e definire la propria password (il nome utente sarà "nomecognome"). L'accesso alla piattaforma avviene tramite un link che rimanda alla pagina di login: https://redcap.dimi.unige.net/redcap/index.php?action=myprojects. I privilegi delle utenze sono sempre settati in modo tale che ogni utente possa vedere solo i dati associati al proprio Centro. Creazione di un database con un interfaccia grafica con la quale i ricercatori inseriscono le informazioni previste dal protocollo, archivio documentale, data cleaning e controlli di qualità, elaborazione statistica.REDCap è una piattaforma web sicura, di seguito i principali aspetti di sicurezza di REDCap: - connessione sicura: REDCap utilizza una connessioni web sicura per proteggere i dati durante il trasferimento. - autenticazione e audit: Include l'autenticazione utente e la registrazione delle attività per monitorare accessi e modifiche ai dati. - conformità: REDCap è progettato per essere conforme a numerosi standard di sicurezza, tra cui HIPAA, 21 CFR Part 11, FISMA, e GDPR. REDCap è una piattaforma con un interfaccia grafica fruibile via browser di EDC (Cattura dati elettronica) guidato dai metadati e con metodologia di flusso di lavoro per progettare la ricerca clinica e raccogliere dati in remoto attraverso dei sistemi di login autorizzati. REDCap permette la modifica dei campi delle variabili per personalizzarle ai fini di uno studio specifico, la gestione e l'elaborazione dei dati a fini statistici, l'archiviazione della documentazione degli studi. Gli accessi con le relative attività sul portale possono essere diversificati a seconda delle richieste del promotore. REDCap fornisce dei certificati di validazione e delle procedure d'uso. La mitigazione dei rischi sopra riportati avviene applicando le seguenti misure di sicurezza a garanzia della riservatezza, disponibilità e integrità dei dati a livello: - organizzativo, tramite ad esempio: istruzioni interne, assegnazione degli incarichi a personale qualificato, formazione agli incaricati del trattamento, profilazione degli accessi a sedi e sistemi informatici; - fisico, tramite ad esempio: gestione degli accessi alle sedi del trattamento, dispositivi di allarme, vigilanza, dispositivi antincendio, dispositivi di controllo di umidità e temperatura, continuità dell'alimentazione elettrica; - logico, tramite ad esempio: gestione delle credenziali di accesso a sistemi e software con password policy di complessità e durata, gestione dei log degli accessi a sistemi e programmi, antivirus centralizzato, firewall perimetrali, ridondanza e virtualizzazione dell'infrastruttura informatica a supporto, backup dei dati, snapshot dei sistemi, ridondanza dei collegamenti di rete, compartimentazione logica delle reti, trasmissione cifrata dei dati, vulnerability assessment periodici.

Tecnologia	REDCap è una piattaforma web sicura, di seguito i principali aspetti di sicurezza di REDCap: - connessione sicura: REDCap utilizza una connessioni web sicura per proteggere i dati durante il trasferimento. - autenticazione e audit: Include l'autenticazione utente e la registrazione delle attività per monitorare accessi e modifiche ai dati. - conformità: REDCap è progettato per essere conforme a numerosi standard di sicurezza, tra cui HIPAA, 21 CFR Part 11, FISMA, e GDPR. REDCap è una piattaforma con un interfaccia grafica fruibile via browser di EDC (Cattura dati elettronica) guidato dai metadati e con metodologia di flusso di lavoro per progettare la ricerca clinica e raccogliere dati in remoto attraverso dei sistemi di login autorizzati. REDCap permette la modifica dei campi delle variabili per personalizzarle ai fini di uno studio specifico, la gestione e l'elaborazione dei dati a fini statistici, l'archiviazione della documentazione degli studi. Gli accessi con le relative attività sul portale possono essere diversificati a seconda delle richieste del promotore. REDCap fornisce dei certificati di validazione e delle procedure d'uso. La mitigazione dei rischi sopra riportati avviene applicando le seguenti misure di sicurezza a garanzia della riservatezza, disponibilità e integrità dei dati a livello: - organizzativo, tramite ad esempio: istruzioni interne, assegnazione degli incarichi a personale qualificato, formazione agli incaricati del trattamento, profilazione degli accessi a sedi e sistemi informatici; - fisico, tramite ad esempio: gestione degli accessi alle sedi del trattamento, dispositivi di allarme, vigilanza, dispositivi antincendio, dispositivi di controllo di umidità e temperatura, continuità dell'alimentazione elettrica; - logico, tramite ad esempio: gestione delle credenziali di accesso a sistemi e software con password policy di complessità e durata, gestione dei log degli accessi a sistemi e programmi, antivirus centralizzato, firewall perimetrali, ridondanza e virtualizzazione dell'infrastruttura informatica a supporto, backup dei dati, snapshot dei sistemi, ridondanza dei collegamenti di rete, compartimentazione logica delle reti, trasmissione cifrata dei dati, vulnerability assessment periodici.
Base dati	Dati clinici originari dei pazienti e referti strumentali e clinici. I dati verranno estratti dalle cartelle cliniche dei pazienti arruolati e registrati sulla eCRF specificamente progettata su REDCap. Alla registrazione del paziente, gli verrà assegnato un numero di studio, per garantire la pseudonimizzazione dei dati. Inoltre, per uniformare la raccolta dati, la eCRF implementata su RedCap sarà condivisa dal promotore con i centri partecipanti con accesso limitato al PI e ai suoi delegati tramite credenziali personali.

Dati trattati dal software nel contesto di utilizzo

Tipologie dei dati gestiti mediante il prodotto software	Sì	No	N.A.
Il software gestisce dati Personali	X		
Il software gestisce categorie particolari di dati personali	X		
Il software gestisce dati relativi a condanne penali e reati		X	
Il software gestisce dati a maggior tutela di anonimato (HIV,IVG,ecc…)		X	
Ambito di gestione del dato	**Sì**	**No**	**N.A.**
Sono gestiti dati relativi a episodi di cura	X		
Sono gestiti dati relativi a pazienti	X		
Sono gestiti dati relativi a dipendenti (in quanto dipendenti dell'Azienda utilizzatrice)		X	
Sono gestiti dati relativi a fornitori		X	
Sono conservati nel sistema documenti (esempio: PDF) che contengono dati personali e categorie particolari di dati personali e/o dati relativi a condanne penali o reati riferiti all'interessato (dati non disaccoppiabili)			X

Rispetto delle misure di sicurezza	Sì	No	N.A.
Il software è integrato con sistemi di sicurezza permettendo la conformità al GDPR necessarie per lo scenario d'impiego cui è destinato: Privacy by design; Privacy by default; minimizzazione; pseudonimizzazione.	X		
Oppure: Il software è parzialmente integrato con sistemi di sicurezza. Tuttavia, è possibile sviluppare dei controlli compensativi che permettono la conformità al GDPR necessarie per lo scenario di impiego cui è destinato.			X
Il software permette l'autenticazione degli utenti basata su tecniche di strong authentication (autenticazione basata su password ed OPT)	X		
Oppure: Il software permette l'autenticazione degli utenti tramite smart card (CNS, ecc.)			X
Sono previste per default tecniche di abilitazione automatica di meccanismi di costruzione di password complesse	X		

Misure minime	Sì	No	N.A.
La componente privata delle credenziali di accesso è di almeno 8 caratteri alfanumerici	X		
È prevista l'obbligatorietà del cambio password al primo accesso	X		
È prevista la modifica obbligatoria della password ogni 3 / 6 mesi	X		
È prevista la disattivazione automatica della password dopo 6 mesi di non utilizzo	X		
È prevista la disconnessione dell'utente in caso di non uso dell'applicativo per un periodo di tempo parametrizzabile	X		
Il software tiene traccia (log accessi e log attività) delle operazioni effettuate tramite applicativo, comprese le attività di sola visualizzazione dei dati, per un tempo parametrizzabile.	X		
Il software permette la profilazione degli utenti (dipendenti autorizzati ad istruire le pratiche e quindi al trattamento dei relativi dati personali) in modo granulare da consentire solo la visibilità necessaria al ruolo svolto.	X		

Rispetto delle misure e degli accorgimenti in tema di amministratori di sistema	Sì	No	N.A.
È prevista la possibilità di creare livelli differenziati di amministrazione del sistema	X		
È previsto un sistema di registrazione (access log) per gli accessi logici degli amministratori di sistema al database di supporto dell'applicativo	X		
Il sistema di access log ha caratteristiche di inalterabilità, completezza e di verifica della integrità dello stesso	X		
L'access log contiene almeno i riferimenti temporali, la descrizione dell'evento che le ha generate, l'identificazione del soggetto che ha compiuto l'accesso	X		
L'access log è conservato in maniera inalterabile per almeno sei mesi	X		

Misure specifiche per categorie particolari di dati personali o dati personali relativi a condanne penali e reati	Sì	No	N.A.
I dati idonei a rivelare lo stato di salute e la vita sessuale/orientamento sessuale sono registrati e conservati separatamente dagli altri dati personali soggetti a trattamenti che non richiedono il loro utilizzo (disaccoppiamento)	X		
Il software consente l'adozione di tecniche di cifratura o di codici identificativi che non esplicitano direttamente il contenuto informativo in relazione alla gestione di dati idonei a rivelare lo stato di salute o la vita sessuale/orientamento sessuale.	X		
Il software consente l'adozione di tecniche di pseudonimizzazione in relazione alla gestione di categorie particolari di dati personali, o dati personali relativi a condanne penali o reati	X		
Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, sono trattati mediante codici identificativi che non esplicitano direttamente il contenuto informativo	X		
Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, o documenti che contengono in modo non divisibile dati personali e categorie particolari di dati personali sono trattati mediante tecniche di cifratura	X		
Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, sono trattati mediante altre soluzioni rispetto alle due precedenti, ai fini della loro temporanea inintelligibilità		X	

Cancellazione dei dati	Sì	No	N.A.
Il sistema consente di definire, per classi di informazioni, il tempo di conservazione in relazione al momento in cui sono state prodotte e al momento in cui è stata raggiunta la finalità per le quali sono state raccolte.	X		
Il sistema consente la cancellazione delle informazioni che hanno raggiunto il tempo limite di conservazione	X		
Il sistema consente di individuare le informazioni relative ad un soggetto (interessato), e in modo puntuale settarle per la cancellazione, il blocco, e l'eventuale ripristino a seguito di blocco	X		
Il sistema dispone di servizi (esempio in collaborazione applicativa) che consentono ad un sistema esterno di individuare le informazioni relative ad un soggetto (interessato), e in modo puntuale settarle per la cancellazione, il blocco, e l'eventuale ripristino a seguito di blocco	X		

ANALISI DEI RISCHI (N.B. limitata al perimetro di diretta gestione dell'E.O. Ospedali Galliera per i trattamenti di propria titolarità)

Preparazione degli elementi utili alla validazione

Elaborazione della sintesi relativa alla conformità al GDPR delle misure che consentono il rispetto dei principi fondamentali

Legenda valutazione

0	1	2	3
Non applicabile	Non soddisfacente	Migliorabile	Soddisfacente

Misure che consentono il rispetto dei principi fondamentali	Valutazione	Eventuali misure correttive previste
Finalità: determinate, esplicite e legittime	3	
Base giuridica	2	Sussistono ipotesi in cui non risulta in concreto possibile acquisire il consenso degli interessati. Nei casi in cui questa impossibilità venga superata, si dovrà procedere alla raccolta del consenso informato.
Minimizzazione dei dati: adeguati, pertinenti e limitati (necessari)	3	
Qualità dei dati: esatti ed aggiornati	3	
Durata della conservazione	3	

Misure a protezione dei diritti degli interessati	Valutazione	Eventuali misure correttive previste
Informazione agli interessati (trattamento legale e trasparente)	2	Sussistono ipotesi in cui non risulta in concreto possibile acquisire il consenso degli interessati. Nei casi in cui questa impossibilità venga superata, si dovrà procedere alla raccolta del consenso informato.

Raccolta del consenso	2	Sussistono ipotesi in cui non risulta in concreto possibile acquisire il consenso degli interessati. Nei casi in cui questa impossibilità venga superata, si dovrà procedere alla raccolta del consenso informato.
Esercizio dei diritti di cui al GDPR	3	
Sub responsabili: identificati e contrattualizzati	0	
Trasferimento dei dati extra-UE nel rispetto del GDPR	0	

Misure riguardanti i dati oggetto di trattamento	Valutazione	Eventuali misure correttive previste
Cifratura/Pseudonimizzazione dei dati trattati	3	
Anonimizzazione dei dati trattati	3	
Controllo degli accessi logici degli utilizzatori	3	
Tracciabilità delle operazioni sui dati	3	
Archiviazione sicura dei dati	3	

Misure generali di sicurezza del sistema dove il trattamento è effettuato	Valutazione	Eventuali misure correttive previste
Continuità operativa (esiste un piano di continuità operativa per i dati trattati)	3	
Protezione da attacchi informatici (utilizzo di antivirus, antimalware, intrusion prevention system)	3	
Gestione delle postazioni lavoro (blocco della postazione quando non presidiata)	3	
Sicurezza dei siti web e sicurezza dei canali informatici utilizzati (protocollo https, firewall, VPN)	3	
Back up e disaster recovery	3	
Modalità di mantenimento server/sistemi/software (aggiornamento del software, del sistema operativo e dell'hardware)	3	

Controllo degli accessi informatici dove sono trattati i dati (autenticazione e profilazione utenti)	3	
Controlli degli accessi fisici ai locali dove sono trattati i dati	3	
Prevista cifratura dei dischi rigidi di server e/o postazioni	3	
Distruzione sicura dell'hardware	3	

Misure generali di sicurezza del sistema dove il trattamento è effettuato	Valutazione	Eventuali misure correttive previste
Organizzazione (il titolare del trattamento ha realizzato e mantiene un'organizzazione interna dei ruoli e delle responsabilità nel trattamento dati personali)	3	
Gestione delle regole (il titolare del trattamento ha realizzato e applica politiche interne in materia di protezione dati personali)	3	
Gestione dei rischi (il titolare del trattamento applica i principi di privacy by design e by default e svolge valutazioni del rischio in riferimento ai trattamenti effettuati)	3	
Gestione del progetto (il trattamento oggetto della presente valutazione è condotto mediante la chiara definizione dei ruoli, delle responsabilità, delle finalità e delle modalità di svolgimento da parte del titolare del trattamento)	3	
Gestione degli incidenti e della violazione dei dati (il titolare del trattamento ha realizzato e applica una procedura interna in materia di data breach)	3	
Gestione del personale (il titolare del trattamento individua al proprio interno le persone autorizzate e le sottopone a formazione periodica in materia di privacy)	3	
Rapporti con i terzi (il titolare del trattamento provvede all'individuazione dei ruoli privacy ricoperti da eventuali soggetti esterni con cui si rapporta, alla stipula degli eventuali accordi di contitolarità e alla nomina dei responsabili ove necessario)	0	
Supervisione e audit (il titolare del trattamento effettua periodicamente verifiche interne e sui responsabili esterni in tema di *compliance* con la normativa in materia di privacy).	3	

VALUTAZIONE DEL RISCHIO

Per garantire una corretta valutazione di seguito vengono riportati gli impatti e la relativa descrizione.

Impatto (I)	Descrizione dell'impatto	Valore
Basso	Gli individui non saranno impattati dalla Violazione o potrebbero essere impattati da alcuni superflui inconvenienti, che saranno in grado di superare senza alcun problema.	1
Medio	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà.	2
Alto	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà.	3
Molto alto	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare.	4

Successivamente si deve valutare la probabilità che l'impatto individuato si verifichi.

Probabilità (P)	Descrizione della probabilità	Valore
Bassa	La minaccia / rischio non si può realizzare	1
Media	È probabile che la minaccia / rischio si realizzi	2
Alta	La minaccia / rischio si verificherà sicuramente prima o poi	3
Molto alta	La minaccia si realizzerà con certezza nel prossimo futuro	4

Specchietto valori probabilità (somma dei valori espressi nelle tabelle relative alle misure di sicurezza applicate)

0	Molto Alta	25	Alta	50	Media	75	Bassa	99

Definiti Impatto (I) e Probabilità (P) e moltiplicando il valore assegnato tramite la formula "IxP" (impatto X probabilità), si otterrà, il livello di rischio associato ad ogni singola minaccia.

Impatto (I)	Probabilità (P)	Livello di rischio associato (I x P)
3	2	6

Il DPIA, quindi si conclude con la valutazione complessiva del rischio associato alle attività di trattamento individuate. La valutazione finale sul rischio si ottiene tenendo in considerazione il valore massimo tra quelli associati alle singole minacce.

Di seguito viene riportato l'intervallo tramite cui è possibile assegnare una classificazione sul livello di rischio ottenuto al termine del DPIA.

Classificazione	Intervallo del rischio
Assenza di Rischio	Valore finale tra 0 e 1 compresi
Rischio Basso	Valore finale tra 2 e 6 compresi
Rischio Medio	Valore finale tra 7 e 11 compresi
Rischio Elevato	Valore finale tra 12 e 16 compresi

Quindi, con riferimento allo specifico trattamento oggetto della valutazione:

Rischi	Descrizione delle principali fonti di rischio	Descrizione degli impatti potenziali	Livello di rischio associato	Accettabile (A)/ Migliorabile (M)
Accesso illegittimo ai dati	Diffusione non autorizzati di dati a seguito di malfunzionamenti o condotta dolosa di soggetti interni o esterni	Violazione della privacy dei pazienti, lesione della dignità personale	3	A
Modifica non desiderata dei dati	Errore nella congruità dei dati a causa di malfunzionamento tecnico o errore umano o intervento doloso	Alterazione dei risultati dello studio	2	A
Perdita dei dati	Distruzione dei dati a causa di malfunzionamento tecnico o errore umano o intervento doloso	Alterazione dei risultati dello studio	2	A
Altri per quanto attiene al perimetro dell'E.O. Ospedali Galliera (specificare)	Nessuno			

Descrizione del piano d'azione (ove necessario)

Misure aggiuntive richieste	Responsabile	Tempo di completamento
n/a		

Valutazioni conclusive

Opinione degli interessati o dei loro rappresentanti (ove raccolta)
Non raccolta.

Parere del Responsabile Protezione Dati (DPO)
Il Responsabile Protezione Dati, esaminata la presente valutazione d'impatto, pur ritenendo che le ipotesi nelle quali si procede ad uno studio senza l'espresso consenso degli interessati dovrebbero essere assolutamente residuali, prende atto delle motivazioni espresse, sotto la propria responsabilità, dalla componente scientifica e sanitaria che l'ha redatta invocando le esenzioni di cui all'art. 110 del D.Lgs. 196/2003 e s.m.i. e delle conseguenti misure applicate a tutela degli interessati. Invita comunque l'Ente e i singoli ricercatori a compiere ogni sforzo necessario per applicare compiutamente, anche in presenza di finalità meritorie quali quelle sottese allo svolgimento delle attività di ricerca, i principi di trasparenza e correttezza verso gli interessati riducendo al massimo il ricorso alle deroghe di cui all'art. 110 Codice privacy. Ciò posto, per quanto riguarda i rischi previsti e le misure di sicurezza applicate allo specifico studio così come descritti nella presente valutazione d'impatto, lo scrivente ritiene che la realizzazione dello studio in questione possa considerarsi compatibile con le previsioni di cui al Regolamento 2016/679/UE limitatamente ai profili di trattamento che ricadono sotto la titolarità dell'Ente. Perplessità destano, invero, alcune modalità di trattamento che si preannunciano nel protocollo con riferimento alle attività che verranno direttamente svolte sotto la titolarità del Promotore. In particolare, appaiono allo stato carenti gli elementi conoscitivi relativi all'impiego di sistemi di intelligenza artificiale e all'eventuale impatto dei relativi output sui protocolli di cura. Si prende comunque atto del fatto che il Promotore ha realizzato sullo studio in questione una propria valutazione d'impatto che si è conclusa con esito positivo e di aver adempiuto alle previsione dell'art. 110 del Codice privacy e, pertanto, non si ritiene di proporre opposizione alla partecipazione allo studio in questione. Lo scrivente si riserva, comunque, di rivedere tale parere all'esito dell'effettiva attivazione dello stesso e nel caso in cui pervengano richieste o segnalazioni in merito da parte degli interessati, delle Autorità competenti/o di terzi.

Validazione della DPIA

Sottoscrizioni	Firma	Data
Il Responsabile Protezioni dati		
Il Titolare del trattamento		

Aggiornamenti successivi:

Data	Aggiornamento

MARIO MAZZEO
15.01.2026
00:35:13
GMT+01:00

FRANCESCO
QUAGLIA
19.01.2026
18:08:18
GMT+01:00