Valutazione d'impatto sulla protezione dei dati (c.d. DPIA) relativa allo Studio "Tools guidati dall'intelligenza artificiale per le malattie aortiche e le comorbidità cardiovascolari (TIA-MAC)"

RAISE Spoke 2, WP 4 Task 4.3 "AI-driven tools for primary aortic diseases and cardiovascular comorbidities".

Titolare del trattamento: Università degli studi di Genova - Dipartimento di scienze chirurgiche e diagnostiche integrate – DISC

Responsabili del trattamento

Responsabile del trattamento per l' Ospedale Policlinico San Martino: Dott. Giuseppe Cittadini

Responsabile del trattamento per l'Ospedale Galliera: Dott. Francesco Paparo

Nome Valutatore:

Direttore DISC – referente privacy: Prof. Carlo Terrone

Responsabile scientifico dello Studio: Prof. Giovanni Spinella

Data di creazione:

I Progetti su studi clinici osservazionali (di seguito "Progetti"), hanno come finalità la generazione di valore e benefici per tutti i pazienti, partecipando attivamente a progetti di ricerca. Questo viene realizzato mediante la predisposizione di strumenti che consentono al personale medico o sanitario di raccogliere in modo sistematico e ordinato dati clinici retrospettivi e prospettici, informazioni sulla qualità della vita e/o risultati riportati direttamente dai pazienti (PROs). Hanno altresì come obiettivo la valorizzazione clinica e scientifica di competenze, processi e dati, attraverso servizi avanzati di estrazione, raccolta e analisi di grandi volumi di dati.

Gli studi e le ricerche condotte nell'ambito di tali Progetti sono valutati e condotti considerando i potenziali benefici in riferimento al miglioramento dei pazienti (es.*dei percorsi di cura per il paziente, ai risultati attesi dalla comunità scientifica e al progresso sociale generato per l'intera collettività*).

1) Nozione di valutazione d'impatto

"Una valutazione d'impatto sulla protezione dei dati (c.d. DPIA) è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli".

2) Quadro normativo

Decreto legislativo 196/2003 e s.m.i, Codice in materia di protezione dei dati personali: Articolo 110;

Garante per la protezione dei dati personali, provvedimento n. 467 dell'11 ottobre 2018 – G.U. 269 del 19 novembre 2018.

3) Soggetti interessati

L'attività dei Progetti interessa il trattamento di dati riguardanti i pazienti assistiti o presso i centri Ospedalieri arruolatori partecipanti allo studio.

4) Valutazione preliminare

4.1 Descrizione del trattamento

La finalità è quella di contribuire a generare valore e beneficio per tutti i pazienti, partecipando attivamente a progetti di ricerca. Questo viene realizzato mediante la predisposizione di strumenti che consentono al personale medico o sanitario di raccogliere in modo sistematico e ordinato dati clinici retrospettivi e prospettici, informazioni sulla qualità della vita e/o risultati riportati direttamente dai pazienti (PROs). Ulteriore obiettivo è la valorizzazione clinica e scientifica di competenze, processi e dati, attraverso servizi avanzati di estrazione, raccolta e analisi di grandi volumi di dati.

Per il raggiungimento di tale finalità il DISC – Dipartimento di scienze chirurgiche e diagnostiche integrate opera mediante i seguenti *asset*:

- **Creazione di *database*** consultabili su piattaforma RED CAP per una rapida visualizzazione dei dati da parte dei ricercatori secondo parametri specifici, ad esempio a seconda della patologia o del gruppo di lavoro;
- ***Data entry*****:** attività di raccolta dati svolta da figure professionali con competenze tecniche, scientifiche, gestionali ed organizzative;
- ***Data registry*****/archivi digitali:** sviluppo, organizzazione e gestione di registri dati/archivi digitali secondo parametri assegnati;
- ***Data Clustering*****:** realizzazione di *dataset* clinici specializzati per patologia.

Lo studio oggetto della presente DPIA consiste in uno studio osservazionale retrospettivo, è spontaneo e no profit.

L'organizzazione dello studio prevede che i centri per la sperimentazione arruolino i pazienti gestendo l'acquisizione del consenso informato e del consenso al trattamento e forniscano al DISC i dati per l'analisi tramite la rete di AI.

I dati sono trasmessi in forma pseudoaninimizzata, così da consentire ai soli centri, e non al DISC, l'associazione dei dati clinici e delle immagini TC all'identificativo del soggetto arruolato.

Per dati si intendono file DICOM delle immagini TC ed informazioni cliniche che si ottengono dalle SDO. I file DICOM delle immagini verranno elaborate, in forma anonima, dalla rete neurale al fine di ottenere parametri geometrici.

4.2 Valutazione della conformità

- **Base giuridica/motivazione legittima del trattamento:**
  - Articolo 110 del Decreto legislativo 196/2003
  - Il trattamento, necessario a fini di ricerca scientifica è effettuato in conformità dell'Articolo 89, paragrafo 1 del suddetto Regolamento, 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.
- **Soggetti che accedono ai dati:** personale incaricato del trattamento e adeguatamente formato da parte del titolare.

- **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.

- **Modalità di raccolta dei dati:** i dati clinici verranno inviati al DISC sotto forma di file excel, successivamente verranno archiviati nella apposita scheda REDCap. I File dicom verranno inviati dai centri reclutatori al DISC. Dopo l'analisi i parametri geometrici verranno aggiunti alla scheda REDCap.

- **Modalità di aggiornamento e eliminazione dei dati:** i dati sanitari pseudonimizzati trattati nell'ambito dei Progetti e caricati su RED CAP potranno essere aggiornati e/o cancellati a seguito di apposita richiesta da parte dell'interessato.

- **Modalità di rilascio dell'informativa agli interessati e richiesta del consenso:** sono consegnate agli interessati direttamente o per mezzo dei Centri ed Enti arruolatori, con la precisazione che il dato verrà trasferito, ai fini dello studio, a Unige in forma pseudoanonimizzata.

- **Trasferimento a soggetti terzi e in Paesi extra Ue:** non previsto.

- **Periodo di conservazione dei dati:** i dati sanitari pseudonimizzati verranno trattati per il tempo previsto dalle normative vigenti in materia di sperimentazioni cliniche e, in particolare, per un periodo non superiore a 10 anni dal momento della raccolta dei dati.

- ***Asset* a sostegno del trattamento:** *hardware*, *software*, archivi e reti sono tutti compresi nel perimetro aziendale e gestiti da personale interno anche a livello di amministrazione dei sistemi. Gli *asset* ricadono dunque sotto le politiche di gestione e sicurezza aziendali.

4.3 Motivi della valutazione d'impatto

La DPIA è stata realizzata per valutare i potenziali rischi che possono derivare dall'attività di trattamento nei confronti degli interessati, così da consentire l'adozione di adeguate misure di sicurezza.

L'esecuzione della DPIA è stata ritenuta necessaria in ragione:

- ♡ del volume e della tipologia di dati utilizzati (dati personali relativi alla salute);
- ♡ dell'ampio numero e della tipologia d'interessati coinvolti (per lo più pazienti e, dunque, suscettibili di poter essere intesi quali soggetti vulnerabili);
- ♡ della durata prolungata dell'attività di trattamento svolta nell'ambito del progetto;
- ♡ delle innovative soluzioni tecnologiche e modalità di analisi impiegate (sistemi di Intelligenza Artificiale, dispositivi *wearable*).

La DPIA è stata inoltre realizzata in ottemperanza alle previsioni dell'Articolo 110 del D.lgs. 196/2003 che individua nell'esecuzione e nella pubblicazione della DPIA uno dei requisiti la cui soddisfazione

rende legittimo il trattamento dei dati relativi alla salute a fini di ricerca scientifica anche senza il consenso dell'interessato.

5) Conduzione della DPIA

5.1 RED CAP - Metodo adottato

Data la sovrapponibilità del trattamento nell'ambito dei Progetti in premessa, sia nella modalità di raccolta che nella modalità di gestione e conservazione dei dati, vengono individuati gli asset relativi alla piattaforma RED CAP. Il processo di analisi dei rischi analizza le vulnerabilità, le relative minacce, e le contromisure, dirette o indirette, attuate, fornendo il livello di rischio. Tale livello tiene anche conto della probabilità e dell'impatto che l'attuazione della minaccia avrebbe sui dati personali trattati, per mezzo degli specifici asset.

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.

L'accesso alla piattaforma avverrà attraverso login

5.2 RED CAP - Identificazione e valutazione dei rischi

Di seguito un estratto del livello di rischio per tipologie di asset, calcolato anche sulla base di vulnerabilità indirette.

Rischio	Software	Luoghi	Organizzazione	Postazionidilavoro	Server	ApparatiRetedati	Storage/Backup	disponibilità	riservatezza	integrità
Malfunzionamento e degrado di apparecchiature	\	\	basso	basso	basso	basso	basso	x		x
Uso non autorizzato di apparecchiature	\	\	\	basso	basso	basso	basso	x	x	x
Furto di apparecchiature	\	\	\	basso	basso	basso	basso	x	x	x
Indisponibilità sistema informativo	basso	\	\	medio	basso	medio	basso	x		

Ingressi non autorizzati ai locali ad accesso ristretto	\	basso	basso	\	\	\	\		x	
Mancanza di alimentazione elettrica	\	medio	medio	medio	basso	medio	basso	x		
Incendio	\	basso	basso	\	\	\	\	x		x
Allagamento	\	basso	basso	\	\	\	\	x		x
Furto di dati	basso	\	basso	medio	basso	basso	medio	x	x	
Modifica non autorizzata di dati	basso	\	basso	basso	medio	basso	basso			x
Presa visione abusiva di dati	basso	\	basso	basso	medio	basso	basso		x	
Mancata accessibilità dei dati	basso	\	basso	basso	basso	basso	basso	x		x
Mancata conservazione dati	basso	\	\	\	\	\	medio	x		x
Malfunzionamento software	basso	\	\	\	basso	\	\	x		x
Uso non autorizzato di software	basso	\	\	\	basso	\	\		x	
Azioni di software suscettibili di arrecare danno	basso	\	medio	basso	basso	medio	medio	x	x	x
Accessi non autorizzati al software	medio	\	\	\	medio	\	\		x	
Errore nello svolgimento di mansioni	\	\	basso	\	\	\	\	x	x	x
Ignoranza procedure di gestione	basso	\	basso	basso	basso	basso	basso	x	x	x

5.3 RED CAP - Mitigazione rischi

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.

5.4 ARCHIVIAZIONE DATI PC UNIGE-DISC - Metodo adottato e mitigazione rischi valutati

I file dicom riferiti alle TC pseudoanonimizzate dei soggetti arruolati verranno archiviati su server dedicati ed installati su rete UniGe.

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 e giustificazioni se non previste	Accettabili (A)/ migliorabili (M)?	Misure correttive
Cifratura	I sistemi di cifratura utilizzati sono a chiave asimmetrica e tipicamente sono mirati alla gestione criptata dei canali http. È quindi utilizzato il sistema di criptatura SSL/TSL con certificati rilasciati dal CA. Non vengono ad oggi utilizzati sistemi di criptatura dei dati sulle basi dati, pur valutandone l'uso futuro sulle sezioni anagrafiche. I dati sono conservati a livello locale su database separato e protetto	**A**	
Pseudonimizzazione	Ad ogni paziente viene assegnato un codice la cui chiave è accessibile al solo ricercatore responsabile dello studio e dallo staff da lui delegato	**A**	
Protezione dei dati in rapporto al sistema utilizzato	I dati anagrafici dei pazienti risiedono in tabelle della base dati logicamente separate rispetto ai dati personali di tipo clinico al fine di ridurre la possibilità di correlazione che viene gestita a livello applicativo (presentazione del dato solo ad utenti autorizzati e debitamente autenticati)	**A**	
Controllo degli accessi logici	Gli accessi alle applicazioni aziendali avvengono solo a seguito di opportuna profilazione sia per quanto attiene l'autenticazione degli utenti attraverso il sistema Active Directory aziendale	**A**	

	utilizzando login e password soggetti a scadenza periodica e criteri di complessità minima, sia per quanto attiene i criteri autorizzativi che sono gestiti direttamente sulle applicazioni ed in particolare sul sistema di gestione autorizzazioni.		
Tracciabilità degli accessi	E' attivo un sistema di log accessi relativo alle diverse sezioni informative relative a dati dei pazienti per cui è sempre possibile risalire alle attività anche di mera visualizzazione effettuate sui dati clinici dei pazienti.	**A**	
Controllo di integrità	E' attivo un sistema di log accessi relativo alle diverse sezioni informative relative a dati dei pazienti per cui è sempre possibile risalire alle attività anche di mera visualizzazione effettuate sui dati clinici dei pazienti.	**A**	
Modalità di archiviazione	Su server aziendale protetto	**A**	
Sicurezza dei documenti cartacei	Chiusura a chiave degli armadi dedicati alla conservazione del materiale cartaceo	**A**	

6) Ruoli Privacy

Titolare del trattamento

Università degli Studi di Genova

Responsabili del trattamento

Responsabile del trattamento per l' Ospedale Policlinico San Martino: Dott. Giuseppe Cittadini

Responsabile del trattamento per l'Ospedale Galliera: Dott. Francesco Paparo

7) Risultati DPIA

Tutto ciò valutato, e soprattutto

- considerata la natura pseudonomizzata dei dati trattati;
- considerato che gli algoritmi di I.A. sono utilizzati nelle ricerche per individuare i fattori di rischio che influenzano la fase diagnostica di una patologia **non attraverso l'individuazione di soggetti a rischio**, ma attraverso la comprensione dei fattori che influenzano l'andamento di una patologia;

si ritiene che il trattamento in esame, allo stato attuale, presenta un grado di rischio basso per i diritti e le libertà degli interessati al trattamento stesso, espresso secondo la scala di valutazione dei rischi adottata.

8) Revisione ed aggiornamento, con riesame di congruità con le esigenze di protezione dei dati

Il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento (Articolo 35, paragrafo 11 del Regolamento UE 2016/679). Il titolare procederà a revisione ed aggiornamento della presente DPIA in corrispondenza dell'introduzione di nuove procedure nell'ambito dei Progetti.

Genova _____

CARLO TERRONE
Università degli Studi di Genova
21.07.2025 14:20:39
GMT+01:00

Il Capo Dipartimento

Prof. Carlo Terrone