IRCCS "Giovanni Paolo II"
PugliaSalute

DATA PROTECTION IMPACT ASSESSMENT
ai sensi dell'art. 35 del Reg. UE 2016/679

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI
STUDI RETROSPETTIVI

Codice	Descrizione
DPIA-001	**Validation of a Prognostic and Predictive Foundation Model-Based AI Test in Breast Cancer – Studio ATARAXIS**

ELABORAZIONE DPIA PER	☒ **Nuova attività trattamento** ☐ Aggiornamento DPIA ☐ Revisione periodica DPIA

SOGGETTI COINVOLTI NELLO STUDIO	
TITOLARE promotore	**Ataraxis AI, Inc.**
Centri partecipanti quali Titolari del trattamento	• Northwell Health, New York, NY, USA • Karmanos Cancer Institute, Detroit, MI, USA • Incheon St. Mary's Hospital, Incheon, Korea • The University Hospital Basel, Switzerland • IRCCS Istituto Tumori "Giovanni Paolo II" Bari, Italy

DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

	• University of Turin, Turin, Italy Ataraxis AI, Inc.
RESPONSABILE DEL TRATTAMENTO	**NA**
COORDINATORE E SPERIMENTATORI	**Coordinatore (Principal Investigator):** Dott. Giuseppe De Palma - S.C. Oncologia Sperimentale e Gestione Biobanca, IRCCS Istituto Tumori "Giovanni Paolo II", Bari **All'interno del working group sono da considerarsi:** • Dott. Francesco Alfredo Zito, SC Anatomia Patologica • Dott.ssa Concetta Saponaro, SC Anatomia Patologica • Dott. Alessandro Rizzo, SSD C.OR.O., Bed Management, Presa in carico, Team multidisciplinari • Dott.ssa Raffaella Massafra, Laboratorio di Biostatistica e Bioinformatica • Dott.ssa Annarita Fanizzi, Laboratorio di Biostatistica e Bioinformatica

FASI DPIA	☒	**Conduzione DPIA**	
	☐	Parere del DPO	
	☐	Validazione del Titolare	
	☐	Consultazione Preventiva	
	☐	Revisione DPIA	
MODALITA' CONDUZIONE	☒	DPIA OBBLIGATORIA	
	☐	DPIA VOLONTARIA	

IRCCS "Giovanni Paolo II"
PugliaSalute

DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

INDICE

Sommario

DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

Informazioni sulla DPIA

La DPIA, acronimo di *Data Protection Impact Assessment*, è una valutazione preliminare, eseguita dal Titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati. In linea con l'approccio basato sul rischio adottato dal Regolamento generale sulla protezione dei dati, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento" può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:
a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

In particolare, preso atto della tipologia di Studio (retrospettivo) in argomento, è condotta e resa pubblica una valutazione d'impatto sulla protezione dei dati, ai sensi dell'art. 35 del Reg. UE 2016/679 ed in forza del combinato disposto degli artt. 9, par. 2, lett. j) del GDPR, 110 e 110 bis, comma 4 del Codice Privacy.

L'art. 110 del D.lgs 196/03, in tema di trattamento di dati personali per ricerca medica, biomedica e epidemiologica, dispone che "Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento.
Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente

comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.

È stato inoltre consultato il Responsabile della Protezione Dati, anche per condividere metodologie, criteri, e per ricevere consulenza in relazione alle decisioni finali.

La presente valutazione contiene:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

ACCETTABILITA' DEL RISCHIO

Tenuto conto della natura, del contesto, delle finalità e dell'ambito di applicazione del trattamento in esame, il **livello di rischio residuo**, considerato accettabile indicato dal Titolare, sentito anche il parere del DPO, è risultato ☒BASSO ☐ MEDIO ☐ ALTO

Di seguito sono illustrati i dettagli della valutazione d'impatto sulla protezione dei dati.

1 Descrizione sistematica del trattamento

1.1 Contesto

Lo scenario sull'utilizzo di test per la scelta del trattamento nel carcinoma mammario è in gran parte rimasto invariato rispetto alle innovazioni dei primi anni 2000. Tramite l'utilizzo di dati di espressione genica (genomica), test come Oncotype DX costituiscono lo standard ma non senza inconvenienti: infatti, sebbene clinicamente validato, la precisione di Oncotype DX lascia spazio a miglioramenti. Inoltre, i tempi di elaborazione piuttosto lunghi, con l'impiego di 3-4 settimane per passare dalla biopsia ai risultati, costituiscono un elemento critico nel trattamento delle pazienti. Inoltre, Oncotype DX è limitato a un gruppo di pazienti con recettori ormonali positivi ed HER2-negativo, non fornendo in questo modo una possibilità di supporto per molti altri sottotipi di carcinoma mammario. Negli ultimi anni, i progressi nella visione grafica e nell'intelligenza artificiale hanno consentito l'estrazione di informazioni significative provenienti da molteplici tipologie di dati complementari e digitali, come quelli della patologia digitale, della radiologia o della cartella clinica elettronica. A differenza di quelli tradizionali, questi nuovi test possono essere progettati per riconoscere i pazienti ad alto e basso rischio, esclusivamente sulla base dei dati di imaging. La società startup Ataraxis ha sviluppato una piattaforma multimodale di proprietà e dispone dei primi prototipi che rendono le prognosi delle pazienti accurate e quasi istantanee. I test di Ataraxis sono stati addestrati e validati retrospettivamente su una coorte di pazienti dell'azienda ospedaliera universitaria NYU Langone Health di New York (USA), mostrando un iniziale riscontro positivo.

Panoramica del trattamento

1.1.1 Quale è il trattamento in considerazione?

Lo studio includerà pazienti con carcinoma mammario che soddisfano i seguenti criteri di inclusione:

- diagnosi di carcinoma mammario invasivo di stadio I-III,
- possesso di vetrini istologici FFPE colorati con ematossilina eosina provenienti da pazienti naive al trattamento, sia da biopsia o da escissione chirurgica,
- esecuzione di un trattamento standard, cioè non hanno partecipato a uno studio clinico che valutava un farmaco sperimentale,
- avere almeno tre anni di follow-up con informazioni sullo stato di recidiva,
- possesso dei dati minimi dalla cartella clinica elettronica necessari per l'elaborazione

Dati clinici

Per fare previsioni accurate e un'analisi robusta dei sottogruppi, saranno utilizzate informazioni cliniche strutturate sui pazienti e sulla loro malattia.

Staging

- Informazioni sulla stadiazione, preferibilmente sotto forma di dimensione del tumore in mm e numero di linfonodi positivi. In alternativa, la stadiazione può essere fornita in formato TNM (ad es. "T1cN1a" o "stadio IIA"). La stadiazione deve essere diagnosticata come clinica (cTNM) o patologica (pTNM)

Istologia e grado del cancro

- Sottotipo istologico invasivo: duttale (IDC) o lobulare (ILC) altro
- Grado: Preferibile il "Sistema di Nottingham". In alternativa, grado basso/intermedio/alto

Biomarcatori tumorali

- ER (preferibile espressione in %, in alternativa: positivo/negativo/equivoco.
- PR (preferibile espressione in %, in alternativa: positivo/negativo/equivoco.
- HER2 (punteggio FISH/IHC).

Genetica

Punteggio di recidiva del test Oncotype (valore tra 0-100) o di MammaPrint o Prosigna

Trattamento somministrato

- Trattamento sistemico

o se il paziente ha ricevuto un trattamento adiuvante, è necessario fornire i nomi dei farmaci.

o se il paziente ha ricevuto un trattamento neoadiuvante, è necessario fornire i nomi dei regimi terapeutici. Se disponibile, fornire informazioni sulla risposta al trattamento.

- Tipologia trattamento chirurgico (mastectomia, lumpectomia) con numero di linfonodi ascellari positivi e linfonodi sentinella.
- Radioterapia: se ricevuta/non ricevuta.

Follow-up

- Data della diagnosi
- Data dell'ultimo follow-up
- Recidiva, progressione o eventi fatali.
- Data dell'evento

- Tipo di evento (recidiva locale/regionale/distante, progressione, morte correlata o meno al carcinoma mammario)

Digitalizzazione dei vetrini
Sarà richiesto almeno 1 vetrino istologico FFPE colorato con ematossilina eosina da biopsia o da procedura chirurgica, relativo a pazienti naive al trattamento. Se la paziente ha ricevuto un trattamento neoadiuvante, solo quello della biopsia sarà accettabile. Se alla paziente è stato fatto il test Oncotype Dx, si selezionerà un vetrino dallo stesso blocchetto utilizzato per l'Oncotype.
I vetrini non saranno trasferiti presso altre strutture esterne ma verranno esclusivamente digitalizzati con un ingrandimento di almeno 20x (preferibile 40x) e inviati presso la società Ataraxis mediante un protocollo elettronico SFTP messo a disposizione dallo stesso Promotore.
Ataraxis eseguirà poi il controllo di qualità manuale e/o automatico sui vetrini scansionati e potrebbe scartare quelli che non soddisfano i requisiti di qualità.

Tipologia di Studio

Studio osservazionale, retrospettivo, multicentrico, no profit.

1.1.2 Quali sono le responsabilità connesse al trattamento?

Gli sperimentatori coinvolti nello Studio sono appositamente autorizzati al trattamento dei dati, ai sensi dell'art. 29 del Reg. UE 2016/679 e dell'art. 2 quaterdecies del Dlgs 196/2003, così come novellato dal D.lgs 101/2018. Nell'ambito dello Studio risulta designata la società Ataraxis AI Inc. quale soggetto terzo in qualità di Responsabili del trattamento dati ai sensi dell'art. 28 del GDPR.

1.1.3 Ci sono standard applicabili al trattamento?

- La linea guida di Buona Pratica Clinica [Good Clinical Practice (GCP)] è uno standard internazionale di etica e qualità scientifica per progettare, condurre, registrare e relazionare gli studi clinici che coinvolgono soggetti umani. La GCP ha l'obiettivo di fornire, in conformità con i principi per la tutela dei diritti dell'uomo stabiliti dalla Dichiarazione di Helsinki, uno standard comune ad Unione Europea, Giappone e Stati Uniti per facilitare la mutua accettazione dei dati clinici da parte delle autorità regolatorie di queste aree geografiche;

- La linea guida recepita dall'Italia (G.U.R.I. n.191 del 18 agosto 1997) è stata messa a punto sulla base delle GCP attualmente adottate da Unione Europea, Giappone e Stati Uniti, oltre che da Australia, Canada, Paesi Nordici e dall'Organizzazione Mondiale della Sanità (OMS);

- Il trattamento di dati personali per scopi di ricerca scientifica è effettuato nel rispetto del Regolamento UE 2016/679, del Codice, delle Prescrizioni relative al trattamento dei dati genetici e delle Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, allegati 4 e 5 al Provvedimento del Garante 5 giugno 2019 (doc. web 9124510), nonché delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica allegato A5 al Codice, che costituiscono condizione essenziale di liceità e correttezza dei trattamenti (art. 2-quater del Codice e art. 21, comma 5 del d.lgs. 10 agosto2018, n. 101)

1.2 Dati, processi e risorse di supporto

1.2.1 Quali sono i dati trattati e gli asset a supporto?

Tipologia di dati personali	Categoria interessati
☒ **Dati identificativi comuni** (es. nome, cognome, indirizzo) ☒ **Dati di contatto** (recapiti email, telefono, cellulare, etc.) ☐ Credenziali di autenticazioni, chiavi di accesso ☐ Dati raccolti da strumenti audiovisivi, videosorveglianza ☐ Dati raccolti da tecnologie traccianti e/o di monitoraggio ☐ Dati raccolti da tecnologie IoT	• Pazienti deceduti o non reperibili • Pazienti in vita (in follow-up)

☐ Dati su abitudini di vita, consumi e comportamento
☐ Dati su familiari/stato familiari
☐ Dati bancari
☐ Dati sulla localizzazione
☐ Dati sulla solvibilità economica

☐ Appartenenza sindacale
☐ Convinzioni politiche, religiose o filosofiche
☐ Origine razziale o etnica
☒ **Dati sulla salute**
☐ Orientamento e vita sessuale
☒ **Dati genetici**
☐ Dati biometrici
☐ Dati "giudiziari" (diritto penale)

Altro:

……

COMPONENTI ORGANIZZATIVE	
Soggetti interni	Lo staff dello studio è composto dal Principal Investigator ed i ricercatori opportunamente individuati in fase di sottomissione dello studio e nel corso dello stesso. Al Principal Investigator viene conferita la delega per la gestione delle attività di trattamento dei dati personali per i compiti relativi alla protezione dei dati personali necessari per la conduzione dello studio. Gli altri componenti dello staff sono autorizzati al trattamento di dati personali da parte del P.I. tramite apposito atto di nomina individuale.
Soggetti esterni	Tra l'IRCCS ed il Promotore i rapporti sono regolati dal protocollo e dal Data Transfer Agreement (DTA)

COMPONENTI TECNOLOGICHE	
Applicazioni	Per l'elaborazione dei dati sono utilizzati sistemi di office automation quali Microsoft Word, Excel
Infrastrutture ICT	Per la conservazione dei dati in formato elettronico sono utilizzati i sistemi di storage aziendali opportunamente protetti sia per quanto riguarda l'accesso fisico che l'accesso ai database che sono opportunamente criptati secondo le regole tecniche usuali e politiche di backup specifiche
Reti informatiche	I computer utilizzati per il trattamento dei dati si trovano su rete dedicata e messa in sicurezza su apposita VLAN. I trasferimenti dei dati avverranno mediante protocollo sftp che utilizza una connessione cifrata ssh.
COMPONENTI FISICHE	
Asset	Per l'elaborazione dei dati sono utilizzati appositi strumenti software aziendali. I PC su cui sono installati tali software sono muniti di idonei sistemi di autenticazione, autorizzazione e tracciabilità delle operazioni
Sedi	Il trattamento dei dati avviene attraverso postazioni di lavoro presso la sede aziendale della ricerca scientifica con accesso riservato
Archivi	I dati personali sono conservati in sicurezza presso l'archivio corrente aziendale o su IaaS (Infrastructure as a Service) in cloud opportunamente protetta.

1.3 Finalità del trattamento

Il trattamento dei dati personali identificativi risulta necessario per la ricerca scientifica e, nel dettaglio, per le seguenti finalità dello Studio:

Obiettivo primario:

- Valutare l'accuratezza dei test Ataraxis nel predire il rischio di recidiva nelle pazienti affette da carcinoma mammario in stadio iniziale.

- Confrontare l'accuratezza dei test Ataraxis con il test standard, Oncotype DX, nel predire il rischio di recidiva nelle pazienti con carcinoma mammario in stadio iniziale HR+ HER2-**.**

Principi Fondamentali

1.4 Valutazione della necessità e proporzionalità del trattamento del trattamento

Il trattamento è effettuato nel rispetto delle prescrizioni previste dall'art. 5 del GDPR e pertanto saranno trattati secondo i principi di:

1. liceità, correttezza e trasparenza
2. limitazione della finalità
3. minimizzazione dei dati
4. esattezza
5. limitazione della conservazione
6. integrità e riservatezza

Lo Studio in argomento comporta il trattamento di dati personali riconducibili allo stato di salute degli assistiti in cura presso l'IRCCS, secondo i criteri di inclusione dello Studio.

1.4.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento correlato allo Studio è effettuato nel rispetto del principio di liceità e trasparenza. A tal proposito è stata predisposta e pubblicata sul sito internet istituzionale, l'informativa Privacy sugli studi retrospettivi. Lo scopo dello Studio è esplicito ed è descritto dettagliatamente nella documentazione di presentazione del medesimo Studio approvato dal Comitato Etico competente.

1.4.2 Quale è il flusso dei dati durante il ciclo di vita del trattamento?

Il ciclo di vita del dato ha origine dall'acquisizione dei dati relativi alla salute dalla documentazione sanitaria e archivi presenti presso la SSD C.Or.O., Bed management, Presa in carico, Team multidisciplinari e la SC Anatomia Patologica dell'IRCCS; successivamente si provvede all'annotazione in un file excel. In un file separato (tabella di transcodifica) saranno conservate le associazioni codice pseudonimizzato (generatore casuale) e nome/cognome del paziente per l'eventuale necessità di dover rintracciare il paziente. I dati raccolti e le scansioni dei vetrini delle pazienti, dopo esser stati pseudonimizzati, saranno trasferiti mediante l'utilizzo di un protocollo sftp che utilizza una connessione cifrata ssh al Promotore dello studio (Ataraxis AI Inc.) che si occuperà dell'elaborazione dei dati.

1.4.3 Quali sono le basi legali che rendono lecito il trattamento?

Basi giuridiche del trattamento di dati
Paziente in vita e rintracciabile

Art. 9 par. 2 lett. a) del GDPR (**acquisizione del consenso**).

Pazienti deceduti o non rintracciabili

Art. 9 par. 2 lett. j) del GDPR e artt. 110-110 bis c. 4 del d.lgs 196/03:

Il trattamento è necessario a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea, ed è condotta e resa pubblica una valutazione d'impatto sulla protezione dei dati.

Il paziente è qualificato come non rintracciabile dopo almeno 3 tentativi (tracciati) di contatto non riusciti.

Ulteriori garanzie:
art. 8, comma 5-bis del d.lgs. n. 288 del 2003

1.4.4 I dati sono esatti e aggiornati?

I dati personali sono acquisiti dagli archivi aziendali con ulteriori controlli interni in caso di omonimie o omocodie.

Qual è il periodo di conservazione dei dati?

Tipologia di dati personali	Tempi di conservazione
Dati pseudonimizzati	I dati pseudonimizzati saranno conservati per **10 anni** dalla conclusione dello Studio, decorsi i quali saranno anonimizzati.
Tabella di corrispondenza Codice ID/Paziente	La tabella di corrispondenza sarà cancellata in modalità permanente decorsi **10 anni** dalla conclusione dello Studio

1.5 Misure a tutela dei diritti degli interessati

1.5.1 Come sono informati del trattamento gli interessati?

Con riferimento ai pazienti viventi, saranno rese le informazioni sul trattamento dei dati **ai sensi dell'art. 13** del Reg. UE 2016/679, nella fase di arruolamento (**modello informativa in allegato**).
A beneficio dei pazienti deceduti (o per quelli irreperibili) sono pubblicate nell'apposita sezione del sito internet istituzionale, le informazioni sul trattamento dei dati, **ai sensi dell'art. 14** del Reg. UE 2016/679. È altresì pubblicato l'informativa al trattamento dei dati personali con relativa valutazione d'impatto.

1.5.2 Ove applicabile: come si ottiene il consenso degli interessati?

Paziente in vita e rintracciabile

Art. 9 par. 2 lett. a) del GDPR

Il consenso, ove possibile, è raccolto dal paziente in fase di arruolamento, tramite l'acquisizione di firma autografa su modello "Consenso Informato Privacy specifico della Ricerca", come dichiarato nel protocollo.

Paziente deceduti/non rintracciabili

Per tale categoria di pazienti, il consenso non può essere raccolto pertanto ci si avvale dell'art. **110 e 110 bis, comma 4 del Codice Privacy, nonché di quanto stabilito dalla legge n. 56 del 29.04.2024.**

1.5.3 Come fanno gli interessati a esercitare i loro diritti?

I diritti dei pazienti di cui agli artt. 15-22 del GDPR sono sempre garantiti nelle modalità indicate nell'informativa ex artt. 13-14 del GDPR rese al momento dell'arruolamento. Altresì sono resi disponibili sul sito internet istituzionale (https://www.sanita.puglia.it/web/irccs/privacy1) i modelli da poter utilizzare per l'esercizio di tali diritti.
I diritti di cui agli articoli da 15 a 22 del Reg. UE 2016/679 riferiti ai dati personali concernenti persone decedute possono essere esercitati dagli aventi diritto del *de cuius*.
Le informazioni sul trattamento dei dati circa gli Studi condotti in assenza del consenso sono rese pubbliche sul sito internet istituzionale, nell'apposita sezione dedicata alla ricerca scientifica,

unitamente alla valutazione di impatto sulla protezione dei dati personali.

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

E' possibile che i dati personali possano essere trasferiti a soggetti di un altro Paese, anche all'esterno dell'Unione Europea, se previsto da un obbligo di legge oppure in assolvimento di obblighi contrattuali verso un Responsabile del trattamento nominato dall'Istituto. I trasferimenti verso paesi extra UE ed organizzazioni internazionali saranno effettuati soltanto nel pieno rispetto del GDPR, anzitutto verificando se quel Paese offra un livello adeguato di protezione dei dati; in mancanza di tale requisito, il titolare o il responsabile del trattamento attuerà le garanzie a tutela dell'interessato previste dal GDPR.

Misure esistenti o pianificate

• **garanzie** (adozione di tecniche di pseudonimizzazione, minimizzazione, implementazione della privacy by design e by default, previsione di procedure volte a testare, verificare e valutare l'efficacia delle garanzie e misure adottate)
• **misure di sicurezza organizzative** (es: norme e procedure che disciplinano l'aspetto organizzativo della sicurezza)
• **misure di sicurezze fisiche** (es: misure di protezione di aree, apparecchiature, dati)
• **misure di sicurezza logiche** (backup, piano di continuità operativa, piano di disaster recovery) sia in relazione al corretto utilizzo degli strumenti elettronici, sia in relazione alla loro gestione e manutenzione

Di seguito le principali misure tecniche applicate, ai sensi dell'art. 32 del Reg. UE 2016/679:

• Antivirus: misure di contenimento dei virus informatici
• Web Application Firewall
• Intrusion detection system sia a livello applicativo che sullo strato dei dati
• Backup dello storage dei dati
• Tecniche di data masking statico e dinamico (pseudonimizzazione, cifratura ed audit dei dati personali)
• Tecniche di segmentazione del dato

• Tracciamento log applicativi e di sistema
• Patch Management su sistemi client/server
• Piani di continuità operativa
• Utilizzo di utenze nominative
• Meccanismi di identificazione ed autenticazione degli utenti
• Password Policy stringenti
• Test di vulnerability assessment e penetration periodici
• Sistemi di autenticazione e di autorizzazione per il personale preposto al trattamento in funzione dei ruoli ricoperti e delle esigenze di accesso e trattamento;
• Procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati ai soggetti designati al trattamento (sperimentatori)
• Sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Misure di sicurezza specifiche per campioni biologici:
Non applicabile

2 Rischi

2.1 Panoramica dei rischi per diritti e libertà

Il processo di ***valutazione del rischio*** parte dalla determinazione dell'impatto sull'interessato (cioè sulla persona fisica a cui il dato si riferisce) in caso di distruzione, perdita, modifica, divulgazione non autorizzata o altri avvenimenti negativi che possono compromettere la sicurezza del trattamento.

L'impatto derivante dalla perdita di una o più delle caratteristiche della sicurezza delle informazioni, ossia riservatezza, integrità e disponibilità, rappresenta la gravità del danno diretto o indiretto causato agli interessati.

Nel valutare i rischi per le libertà e diritti degli interessati, però, come suggerisce la norma ISO/IEC 29134 si dovrebbero considerare anche altri aspetti, oltre alla sicurezza dei dati; e che pertanto devono essere considerati gli effetti complessivi del trattamento.

I rischi pertanto sono identificati in base ai seguenti quattro parametri:

1) conformità ai principi applicabili al trattamento dei dati (art. 5 del Reg. UE 2016/679)
2) riservatezza
3) integrità

4) disponibilità.

A tal fine, nella determinazione del livello di impatto sono incluse valutazioni sulle possibili conseguenze derivanti da mancanza di trasparenza, mancato rispetto dei tempi di conservazione dei dati, o dalla violazione degli altri principi fondamentali applicabili alla protezione dei dati personali.

- **Quali sono le principali minacce che potrebbero concretizzare il rischio?**

Una minaccia potrebbe concretizzarsi solo al momento dell'acquisizione dei dati durante la consultazione della documentazione sanitaria, che però è effettuata da personale esercente la professione sanitaria, tenuta al segreto professionale, ed istruita in materia di protezione dei dati personali.

- **Quali sono le fonti di rischio?**

Una fonte di rischio potrebbe essere rappresentata dalla tabella di transcodifica che è gestita separatamente e che se sottratta insieme al database centralizzato dello Studio, consentirebbe di risalire allo stato di salute ed alle patologie dei soggetti inclusi nello Studio.

Non si ravvisano rischi per l'assistito in merito alla perdita di disponibilità del dato in quanto, in caso di evento avverso, non saranno compromessi i dati acquisiti e conservati per finalità di diagnosi, assistenza e cura. Anche in caso di perdita di integrità, non saranno compromessi dati acquisiti e conservati per finalità di diagnosi, assistenza e cura, ma solo per la finalità dello Studio.

- **Quali misure fra quelle individuate contribuiscono a mitigare il rischio?**

Oltre alle istruzioni operative fornite agli sperimentatori, è implementato un sistema crittografico sull'archivio centralizzato che prevede crittografia AES 256 bit con 14 round o cicli di elaborazione crittografica.

- **Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?**

Il rischio residuo calcolato, dopo l'adozione delle misure di sicurezza pianificate, è BASSO.

Le fonti di rischio possono essere categorizzate in:

- **Violazioni dei principi applicabili ai trattamenti di dati personali**
- **Minacce alla sicurezza dei trattamenti**

- **Eventi con danni fisici/materiali**
- **Eventi naturali**
- **Perdita o indisponibilità di servizi essenziali**
- **Compromissione di dati e informazioni**
- **Problemi tecnici**
- **Azioni non autorizzate**
- **Compromissione di funzioni / servizi per errori o azioni malevole**

Il livello di rischio è direttamente proporzionale alla probabilità che si verifichino le diverse minacce e alla gravità dell'impatto per gli interessati. Può essere mitigato con l'applicazione delle necessarie misure di mitigazione.

Se l'applicazione delle misure di mitigazione riduce il livello di rischio, fornendo un primo livello di rischio residuo, il governo dei processi e il presidio di controlli efficaci può fornire un ulteriore livello di ponderazione. Ecco perché oltre alle specifiche contromisure, la metodologia utilizzata inserisce, mediante un self assesment, degli obiettivi di controllo specifici per diverse categorie e ambiti, e dei controlli sullo svolgimento del processo di Valutazione di impatto.

Per la data protection si fa riferimento ai controlli della ISO/IEC 29151, estensione di quelli della ISO/IEC 27001 Annex A, a quelli della ISO/IEC 27701:2019 e della ISDP10003:2018.

2.2 Accesso illegittimo ai dati

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

Danno immateriale, perdita dignità, perdita di controllo sui propri dati personali, irritazione, perdita della fiducia nella sanità pubblica, perdita finanziaria

2.2.2 Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accessi esterni non autorizzati, Uso improprio del software, Corruzione dei dati, Comunicazione illegale dei dati e dei documenti, Uso non autorizzato dei dati, attacco hacker.

2.2.3 Quali sono le fonti di rischio?

Fonti di rischio umane interne, fonti di rischio umane esterne

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

Crittografia AES 256 bit sugli archivi elettronici dello Studio e dei relativi backup, Controllo degli accessi logici, Tracciabilità, Lotta contro il malware, Gestione postazioni, Politica di tutela della privacy, Firewalling, EDR.

2.2.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Significativa. La gravità del rischio potenziale di accesso illecito ai dati è stimata come ALTA, in considerazione della tipologia di dati raccolti.

2.2.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

La probabilità di accadimento è stimata come BASSA in considerazione delle misure di garanzia implementate con particolare riferimento alle tecniche di pseudoanonimizzazione e crittografia applicate.

2.3 Modifiche indesiderate dei dati

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

Modifiche ai dati raccolti per finalità di ricerca non comportano un impatto diretto all'interessato.

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

Accessi esterni non autorizzati, Azione di virus informativi o di codici malefici, Uso non autorizzato dei dati, Sabotaggio, Alterazione dolosa o colposa dati

2.3.3 Quali sono le fonti di rischio?

Fonti di rischio umane interne, fonti di rischio umane esterne

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

Crittografia, Controllo degli accessi logici, Tracciabilità, Lotta contro il malware, Gestione postazioni, Backup, Manutenzione, Politica di tutela della privacy

2.3.5 Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitata. La gravità del rischio potenziale di modifica illecita dei dati è stimata come BASSA, in considerazione della presenza di dati originali già raccolti per finalità di diagnosi e cura.

2.3.6 Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

La probabilità di accadimento è stimata come BASSA in considerazione delle misure di garanzia implementate.

2.4 Perdita di dati

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

Perdita di fiducia, irritazione, perdita reputazione, perdita di controllo sui propri dati personali

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

Azione di virus informativi o di codici malefici, Sabotaggio, attacco hacker, Uso non autorizzato dei dati, Uso improprio del software, Accessi esterni non autorizzati

2.4.3 Quali sono le fonti di rischio?

fonti di origine naturale, fonti di rischio umane esterne, fonti di rischio umane interne

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

Backup, Disaster Recovery plan, Manutenzione, Politica di tutela della privacy, Controllo degli accessi logici, Crittografia, Tracciabilità, Lotta contro il malware.

2.4.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

La probabilità di accadimento è stimata come BASSA in considerazione delle misure di garanzia implementate.

2.5 METRICHE PER ANALISI RISCHIO

Valori dei livelli di rischio

Livello	Descrizione
BASSO	Il rischio per gli interessati è accettabile dall'organizzazione mediante misure organizzative e tecniche idonee, ma deve

	continuare ad essere monitorato per controllare che cambiamenti non incrementino il livello di rischio
MEDIO	Il rischio medio per gli interessati potrebbe essere accettabile ma l'adozione delle misure tecnico-organizzative deve essere monitorata su base regolare, e il trattamento può essere sottoposto a ulteriori considerazioni
ALTO	Il rischio per le persone interessate al trattamento è ad un livello non accettabile e necessita un rafforzamento delle misure di mitigazione
ELEVATO	Il rischio per gli interessati si presenta elevato o molto critico, mantenendo un livello non accettabile per l'organizzazione e necessitando l'aggiunta di ulteriori controlli a prevenzione/mitigazione dello stesso

Valori dei livelli di probabilità

Livello	Descrizione
BASSO	Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia si concretizzi in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore
MEDIO	Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore
ALTO	Evento/Minaccia probabile; è un evento che si è già verificato o che può verificarsi con frequenza superiore rispetto alla media con riferimento alle tendenze riportate da studi, ricerche, statistiche di settore

Valori dei livelli di impatto

Livello	Descrizione

IRRILEVANTE	Gli interessati possono incontrare alcuni piccoli inconvenienti, che supereranno senza troppi problemi
LIMITATO	Gli interessati possono incontrare disagi significativi, che riusciranno comunque a superare a dispetto di alcuni problemi
SIGNIFICATIVO	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà
CRITICO	Gli interessati possono avere conseguenze gravi, o addirittura irreversibili, che potrebbero non superare

3 Panoramica dei rischi

Rischio Privacy	Descrizione delle conseguenze per gli interessati derivanti dalla vulnerabilità del trattamento	Livello di impatto
Perdita dei dati personali	**La perdita dei dati potrebbe comportare un danno agli interessati in termini di perdita di controllo sui propri dati**	**MEDIO**
Distruzione non autorizzata o indisponibilità	**La distruzione dei dati o l'indisponibilità degli archivi dello Studio non comporta un impatto diretto sugli interessati**	**BASSO**
Modifica non autorizzata	**La modifica dei dati per finalità di ricerca non comporta un impatto diretto sugli interessati**	**BASSO**
Divulgazione non autorizzata	**La divulgazione di dati personali dei partecipanti allo Studio potrebbe comportare un danno rilevante agli interessati**	**ALTO**

Accesso ai dati non autorizzato	**L'accesso illecito ai dati personali dei partecipanti allo Studio potrebbe comportare un danno rilevante agli interessati**	**ALTO**
Eccessiva raccolta di dati personali	**Utilizzare più dati personali del dovuto implicherebbe un'esposizione di dati personali all'utilizzo per scopi non pertinenti e non compatibili**	**BASSO**
Collegamenti o raffronti inappropriati o non autorizzati a dati personali	**Collegamenti o raffronti con altre banche dati potrebbe comportare danni immateriali agli interessati**	**BASSO**

Rischio Privacy	Descrizione delle conseguenze per gli interessati derivanti dalla vulnerabilità del trattamento	Livello di impatto
Perdita di controllo dei dati da parte degli interessati	**La mancanza di trasparenza e sicurezza dei trattamenti potrebbe comportare un impatto per gli interessati**	**BASSO**
Riuso per finalità diverse dei dati personali senza la consapevolezza e/o il consenso degli interessati	**I dati personali potrebbero essere utilizzati per altre finalità sconosciute all'interessato con danno immateriale agli interessati (mancanza di trasparenza e consenso)**	**BASSO**

Disequità o difettosità dell'elaborazione o del processo	**In caso di errata elaborazione delle informazioni, errori di registrazione etc. gli interessati potrebbero subire nocumento**	**BASSO**
Conservazione immotivatamente prolungata dei dati personali	**La conservazione dei dati oltre il periodo prestabilito e motivato potrebbe comportare un danno immateriale agli interessati**	**BASSO**
Inesattezza o perdita di qualità dei dati personali	**Eventuali inesattezze o perdita della qualità dei dati raccolti non presenta un impatto diretto sui pazienti**	**BASSO**
Re-identificazione dei soggetti interessati	**Il processo di anonimizzazione potrebbe non eliminare la probabilità di re-identificazione dei partecipanti allo Studio, con particolare riferimento a malattie rare, con conseguente nocumento agli interessati**	**BASSO**

DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

CATEGORIE DI MINACCE CONSIDERATE	Livello MAX Prob.
Minacce alla conformità del trattamento	BASSO
Eventi con danni fisici	BASSO
Eventi naturali	BASSO
Indisponibilità dei servizi essenziali	BASSO
Violazioni di dati per azioni deliberate	MEDIO
Problemi tecnici	BASSO
Violazioni di dati per azioni involontarie	BASSO

CATEGORIE DI MINACCE	EFFICACIA MISURA ESISTENTE
Minacce alla conformità del trattamento	MISURE ESISTENTI ADEGUATE
Eventi con danni fisici/materiali/immateriali	MISURE ESISTENTI ADEGUATE
Eventi Naturali	MISURE ESISTENTI ADEGUATE
Indisponibilità di Servizi essenziali	MISURE ESISTENTI ADEGUATE
Compromissione di dati e informazioni per azioni deliberate	MISURE ESISTENTI ADEGUATE
Problemi tecnici	MISURE ESISTENTI ADEGUATE
Compromissione di dati o servizi per azioni involontarie	MISURE ESISTENTI ADEGUATE

DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

A seguito della ponderazione del livello di rischio calcolata mediante l'applicazione della mitigazione delle misure tecniche ed organizzative, il **rischio residuo** risulta **BASSO**, pertanto

ACCETTABILE ☒	**NON ACCETTABILE ☐**

La presente DPIA:

a) essere pubblicata obbligatoriamente è resa pubblica sul sito internet istituzionale nell'apposita sezione della Ricerca Scientifica (pubblicazione obbligatoria se lo Studio rientra nell'ambito del programma di ricerca nazionale, ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502)
b) resa disponibile su istanza degli interessati.

Bari, 21.06.2024