VALUTAZIONE DI IMPATTO

SULLA PROTEZIONE DEI DATI (VIP)

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

trattamento dei dati personali, relativi alla salute, inerenti alla Rete Oncologica Campana e alla Piattaforma web appositamente sviluppata per conseguire gli obiettivi di prevenzione, diagnosi e cura dei tumori maligni.

INDICE

1. CONTESTO DEL TRATTAMENTO

1.1 TRATTAMENTO ESAMINATO

Il presente documento - di seguito denominato VIP (Valutazione d'Impatto sulla Protezione dei dati personali) o anche DPIA (Data Protection Impact Assessment) - esamina il trattamento dei dati personali, relativi alla salute, inerenti alla Rete Oncologica Campana (ROC) e alla Piattaforma web (di seguito denominata anche "Piattaforma ROC" o "Piattaforma") appositamente sviluppata per conseguire gli obiettivi di prevenzione, diagnosi e cura dei tumori maligni.

Il trattamento preso in considerazione riguarda l'intero ciclo di vita dei dati con specifico riferimento alle attività di raccolta, elaborazione, conservazione e cancellazione.

1.2 TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è l'Istituto Nazionale Tumori IRCCS "Fondazione G.Pascale" (di seguito denominato anche solo: "IRCCS PASCALE" o "FONDAZIONE PASCALE") in persona del suo legale rappresentante p.t., con sede legale in Napoli, alla via Mariano Semmola, 42,
in persona del suo l.r.p.t.

La FONDAZIONE PASCALE, in quanto IRCCS, è un Ente del Servizio sanitario nazionale che persegue, secondo standard di eccellenza, finalità di ricerca, soprattutto clinica e traslazionale, nel campo biomedico e in quello dell'organizzazione e gestione dei servizi sanitari e garantisce prestazioni di ricovero e cura di alta specialità (art.1 d.lgs. 16/10/2003, n. 288).

Il presente documento, riconducibile alla FONDAZIONE PASCALE, quale Titolare del trattamento, è stato predisposto, tramite supporto consulenziale esterno, previa notifica al DPO interno, gli AdS, il dip. IT e gli altri Referenti e Collaboratori, interni ed esterni all'Organizzazione, di seguito indicati:

- Sandro Pignata - Responsabile scientifico rete oncologica campana

- Elisabetta Coppola - Responsabile struttura di coordinamento rete oncologica
- Rocco Saviano - Responsabile servizi informatici
- Fabrizio Caccavallo - Responsabile servizi informatici
- Davide D'errico – Case manager.

1.3 DEFINIZIONI

1.3.1 Ai fini della presente VIP si applicano le definizioni di cui al Reg. UE 2016/679 (GDPR) e del D.Lgs. 30/06/2003, n. 196 (Codice in materia di protezione dei dati personali).

1.3.2 Le ulteriori definizioni

a) "VIP" (Valutazione d'Impatto sulla Protezione dei dati personali) o "DPIA" (Data Protection Impact Assessment),

b) "IRCCS PASCALE" o "FONDAZIONE PASCALE",

c) "Rete Oncologia Campana" o "ROC",

d) "Piattaforma ROC" o "Piattaforma",

verranno utilizzate alternativamente per indicare, rispettivamente:

a) il presente documento,

b) l'Ente cui detto documento è riconducibile,

c) la Rete Oncologica Campana,

d) la Piattaforma sviluppta e gestita per conseguire gli obiettivi della ROC.

1.4 CONTESTO INTERNO ED ESTERNO DEL TRATTAMENTO: istituzione della Rete Oncologica Campana (ROC) e implementazione della relativa Piattaforma web

La **FONDAZIONE PASCALE**, tenuto conto del Decreto n. 98/2016 della Regione Campania, istitutivo della rete Oncologica Campana ("Decreto"), ha sviluppato una Piattaforma web per includere tutte le strutture presenti sul territorio regionale competenti per la prevenzione, diagnosi, cura e riabilitazione dei tumori maligni (di seguito anche soltanto: "Centri partecipanti") .

Gli scopi principali della Piattaforma sono:

- ottimizzare la presa in carico e i percorsi di cura dei pazienti nella gestione delle patologie neoplastiche;

- garantire la continuità di cura con un rapido invio delle richieste verso le strutture sanitarie preposte per i servizi domiciliari territoriali.

Ulteriori obiettivi della Piattaforma, funzionali al raggiungimento dei suindicati scopi principali, sono:

consentire a tutti i Centri che fanno parte della ROC, per i rispettivi ambiti di competenza, di contribuire all'attuazione di percorsi assistenziali, organizzati ed efficienti;

assicurare una gestione multidisciplinare integrata;

garantire il rispetto dei principi di appropriatezza ed equità di accesso alle cure.

La Regione Campania, con il citato DCA n. 98/2016 individuava gli organi costitutivi della ROC nei Centri Oncologici di Riferimento Polispecialistici (CORP) con funzioni diagnostico/stadiative, terapeutiche e di follow-up oncologico e nei Centri Oncologici di Riferimento Polispecialistici Universitari o a carattere Scientifico (CORPUS) a cui, oltre alle funzioni già affidate ai CORP, venivano attribuite altre funzioni peculiari (ricerca, formazione, sviluppo di metodi e strumenti, screening, terapia del dolore).

La ROC nasceva dalla necessità di migliorare la gestione dei pazienti oncologici nella Regione Campania, creando un sistema informativo condiviso che permettesse la comunicazione in tempo reale tra i vari nodi della rete.

Con successiva nota prot. n. 731 del 10/2/2017, la Regione Campania affidava alla FONDAZIONE PASCALE il Coordinamento centrale altamente specialistico di tutti i Centri coinvolti nella ROC.

Con successivo DCA n. 43 del 07.06.2019, la Regione Campania illustrava la propria programmazione relativa, in particolare, alla "*Linea progettuale 6 – Reti Oncologiche",* elaborando uno specifico progetto (DCA 43/2019 "*l'infrastruttura della Rete Oncologica Campana deve garantire la piena attuazione di un percorso assistenziale organizzato ed*

efficiente, avversando le prestazioni casuali") in base al quale la ROC doveva operare secondo un articolato modello di governance e realizzare una piattaforma informatica per la consultazione-condivisione dei dati e documenti clinico-sanitari di tutti i pazienti oncologici presi in carico dalla stessa ROC affinchè il sistema, interoperando con tutti i *repository* aziendali, consentisse ai diversi attori dei GOM (aziendali e interaziendali) di accedere al set di informazioni complete, storiche ed aggiornate, del paziente oncologico e anche il passaggio della presa in carico da un GOM all'altro.

L'obiettivo era la gestione e il monitoraggio della domanda oncologica nell'ambito dei PDTA e il potenziamento della connessione tra GOM e CORP/CORPUS.

Alla **FONDAZIONE PASCALE** veniva affidata la funzione di coordinamento delle Aziende.

Pertanto, l'IRCCS PASCALE, ai sensi della richiamata programmazione regionale, predisponeva e metteva in atto documenti e misure tecniche e organizzative ("Accordo Partenariato DCA 43-2019 - Ex art. 15 L. 241.90" e Piattaforma Informatica distribuita della ROC Progetto Esecutivo) volti a realizzare i suindicati obiettivi e a potenziare l'interconnessione tra Rete Oncologica Campana (ROC) e Medici di Medicina Generale (MMG), per garantire il rapido accesso del paziente oncologico al percorso più appropriato.

Negli anni, venivano sviluppati numerosi percorsi Diagnostico Terapeutici Assistenza (PDTA) di patologia, integrati da ulteriori specialisti, con la partecipazione attiva anche dei medici di medicina generale.

Lo sviluppo della ROC permetteva la significativa riduzione di tempi di diagnosi e di inizio delle terapie posto che i MMG potevano segnalare i pazienti e indirizzarli in tempi brevissimi verso la visita dei Gruppi Oncologici Multidisciplinari (GOM) ritenuti più idonei. Ciò consente di avviare il paziente al percorso diagnostico terapeutico condiviso entro soli sette giorni dalla segnalazione, garantendo un accesso rapido e tempestivo alle cure necessarie, nelle fasi di inizio del percorso e di follow-up.

Allo stato, si registra un significativo incremento del numero di MMG che hanno fatto richiesta delle credenziali di accesso alla Piattaforma ROC in tutte le aziende sanitarie e,

successivamente, un aumento del numero di pazienti segnalati alla rete.

Il progetto è stato rafforzato ed esteso ad altre aree territoriali, il numero di MMG coinvolti è notevolmente aumentato e ogni settimana circa 20 nuovi pazienti vengono indirizzati dalla medicina generale ai GOM della Regione.

1.5 OGGETTO DELLA VIP - DESCRIZIONE SISTEMATICA DEL TRATTAMENTO (art. 35, par. 7, lett. a) Reg. UE 2016/679).

L' IRCCS PASCALE ha strutturato la Piattaforma ROC per la raccolta dati, appositamente customizzata, idonea ad effettuare un attento controllo sulla qualità dei dati raccolti in tempo reale e la relativa elaborazione statistica, all'interno della quale vengono inseriti i dati dei pazienti oncologici raccolti dai professionisti sanitari dei Centri Partecipanti.

La gestione della Piattaforma è interna alla FONDAZIONE PASCALE.

L'accesso è ad uso esclusivo del personale previamente autorizzato.

I dati personali (in particolare, di carattere medico/clinico: fattori prognostici, terapie farmacologiche, dati strumentali) delle persone reclutate vengono raccolti prima del trattamento, tramite visite mediche e accertamenti diagnostici e, una volta raccolti, sono trattati (consultati, registrati, conservati, modificati) con logiche strettamente correlate alle finalità del trattamento, applicando misure idonee a garantire la riservatezza, l'integrità e la disponibilità dei dati e osservando i principi *privacy by design* e *by default* di cui all'art. 25 GDPR.

1.5.1 Descrizione funzionale del trattamento

a) Primo contatto con il paziente – raccolta e registrazione dei dati

I pazienti vengono indirizzati alla Piattafiorma dai propri medici di Medicina Generale (MMG), da medici di I livello di Centri oncologici di II livello o da medici dell'ASL nella fase definita "Segnalazione": i citati professionisti, utilizzando credenziali di accesso alla piattaforma ROC, possono creare nuove schede ROC ricercando i pazienti nella Piattaforma tramite informazioni anagrafiche.

In questa fase i dati vengono raccolti e registrati nella Piattaforma.

Ai pazienti registrati in piattaforma ROC vengono spiegati e forniti due documenti: l'informativa per la Presa in carico dai GOM; il consenso informato per lo Studio della ROC: Oncocamp.

b) Presa in carico del paziente, riunione multidisciplinare e refertazione – organizzazione, consultazione, raffronto, elaborazione e utilizzo dei dati

Nella successiva fase di presa in carico del paziente avviene l'integrazione tra più professionisti.

Il case manager, con le proprie credenziali di accesso alla piattaforma ROC, prenota la visita, verifica che i dati inseriti nella scheda paziente siano completi, lo conduce alla visita multidisciplinare e segue il percorso diagnostico terapeutico come previsto nei PDTA.

Il paziente effettua la prima visita necessaria per l'inquadramento del problema presso un ambulatorio dedicato entro 7 giorni dalla segnalazione.

La riunione multidisciplinare del GOM avviene in maniera sistematica e calendarizzata.

Il referto del GOM è un documento che attesta, dopo la valutazione del gruppo multidisciplinare, la miglior indicazione diagnostico-terapeutica; **il verbale** è composto dall'anagrafica, patologie concomitanti, terapie in corso ed anamnesi oncologica del paziente compilati dal case-manager o dal medico proponente; durante il GOM vengono segnalati nel referto le valutazioni, l'indicazione e il programma; una volta completato, il referto, con l'effettiva indicazione terapeutica, viene stampato e firmato dai membri che hanno discusso il caso.

Il case manager dopo la conclusione carica i referti sulla Piattaforma per renderli disponibili per i MMG e medici invianti.

c) Chiusura scheda – consultazione, elaborazione e conservazione.

La scheda della Rete Oncologica Campana di ogni paziente deve essere chiusa con l'indicazione finale del GOM e il case manager ha il ruolo di chiuderla e di compilare gli indicatori richiesti (aperta la schermata e selezionata la voce "chiusura" il case manager procede alla compilazione degli indicatori richiesti).

1.5.2 Sintesi del ciclo di vita dei dati personali

Le attività di raccolta dei dati personali vengono eseguite presso i Centri partecipanti (strutture ospedaliere o universitarie ed istituti di ricerca) avvalendosi di personale qualificato e di mezzi e spazi idonei.

Le informazioni medico/cliniche raccolte sono trasmesse alla **FONDAZIONE PASCALE** mediante l'utilizzo della Piattaforma.

Il personale addetto al caricamento dati del Centro partecipante può visualizzare esclusivamente i dati del proprio Centro e aggiungerli e modificarli in modo tracciabile.

Il periodo di conservazione dei dati personali è strettamente correlato alla necessità di perseguire le finalità della ROC e di costruire analisi e studi futuri volti a migliorare le conoscenze e la pratica clinica nel settore delle patologie oggetto della ROC.

Trascorso detto periodo i dati personali saranno completamente anonimizzati.

1.6 RUOLI SOGGETTIVI IN MERITO ALLA PROTEZIONE DEI DATI PERSONALI

La Regione Campania, con il DCA n. 98/2016 "Istituzione della Rete Oncologica Campana", individuava gli organi costitutivi della ROC nei:

- Centri Oncologici di Riferimento Polispecialistici (CORP)

con funzioni diagnostico/stadiative, terapeutiche e di follow-up oncologico;

- Centri Oncologici di Riferimento Polispecialistici Universitari o a carattere Scientifico (CORPUS) a cui, oltre alle funzioni già affidate al CORP, venivano attribuite altre funzioni peculiari (ricerca, formazione, sviluppo di metodi e strumenti, screening, terapia del dolore);

- **CENTRI ONCOLOGICI presso le ASL** e le strutture per le cure palliative

Con successiva nota prot. n. 731 del 10/2/2017, la Regione Campania affidava alla FONDAZIONE PASCALE il Coordinamento centrale altamente specialistico di tutti i Centri complementari coinvolti nella ROC.

1.6.1 Ciò premesso, in ragione delle finalità istituzionali attribuite, del vigente quadro normativo e regolatorio, nazionale e regionale, e dell'analisi del flusso effettivo dei dati

personali (condotta tenendo conto degli artt. 4, 24, e 32 Reg. UE 2016/679 e dei Considerando 39, 74, 78, 83 nonché delle Linee Guida EDPB 7/2020) **i ruoli soggettivi inerenti al trattamento dei dati personali relativi alla ROC possono essere così individuati**:

1.6.1.1 TITOLARI DEL TRATTAMENTO

Titolari autonomi del trattamento, ciascuno nell'ambito di propria competenza:

- **i Centri Oncologici di Riferimento Polispecialistici (CORP):**

con funzioni diagnostico/stadiative, terapeutiche e di follow-up oncologico

- **i Centri di Riferimento Regionali (CORPUS)**

che oltre alle funzioni dei CORP hanno ulteriori specifiche funzioni (ricerca, formazione, sviluppo di metodi e strumenti, screening, terapia del dolore).

- i Centri Oncologici presso le ASL e le strutture per le cure palliative (Hospice e reparti/ambulatori di Terapia del Dolore)

La FONDAZIONE PASCALE, rientrando nella categoria dei CORPUS, deve ritenersi, nell'ambito di tale ruolo e definizione, un autonomo Titolare del trattamento.

In considerazione di eventuali successivi cambiamenti nel contesto normativo e regolatorio, nel flusso effettivo dei dati e nel potere di decidere mezzi e finalità del trattamento, i Centri partecipanti alla ROC e la FONDAZIONE PASCALE potrebbero essere qualificati Contitolari del trattamento stesso.

1.6.1.2 RESPONSABILI DEL TRATTAMENTO

Alla **FONDAZIONE PASCALE** veniva affidato lo sviluppo e la gestione dell'infrastruttura tecnologica della Piattaforma web della ROC che fornisce supporto tecnologico e informatico per agevolare la comunicazione tra i diversi soggetti della ROC permettendo lo scambio di documenti, dati e informazioni tra gli stessi.

Nell'ambito delle finalità della ROC e della relativa Piattaforma la **FONDAZIONE PASCALE** ne garantisce la gestione amministrativa, tecnica ed informatica.

Pertanto, l'IRCCS Pascale fornisce, attraverso la realizzata Piattaforma, supporto tecnologico e informatico per agevolare la comunicazione tra i diversi soggetti della ROC

al fine di consentirne lo scambio di documenti, dati e informazioni e, nello svolgimento di queste attività, agisce in qualità di Responsabile del trattamento, come indicato nell'atto di informativa che richiama la designazione della FONDAZIONE PASCALE ai sensi dell'art. 28 GDPR da parte di ciascuno dei Titolari sopra richiamati.

1.6.1.3 SOGGETTI "INTERNI" ALLE SINGOLE ORGANIZZAZIONI coinvolti nel trattamento - autorizzati e designati al trattamento

L'attività di trattamento coinvolge, come sopra rilevato, tutti i Centri partecipanti alla ROC con sede in Campania , in qualità di titolari autonomi del trattamento.

Esaminato questo contesto del trattamento, esterno alla FONDAZIONE PASCALE, occorre individuare i ruoli soggettivi in tema di *data protection* del personale individuato per la raccolta e, in generale, per il trattamento e, in particolare, dei MMG.

In linea generale, i dati personali contenuti nella Piattaforma ROC sono trattati dalla FONDAZIONE PASCALE e dagli altri Titolari del trattamento nel rispetto dei principi di cui all'art. 5 Reg. UE 2016/679, mediante soggetti appositamente individuati dai Titolari, in conformità agli artt. 29 GDPR e 2-quaterdecies D.L.gs. 196/03 e sottoposti a regole di condotta analoghe al segreto professionale, qualora non siano tenuti per legge al segreto professionale.

I soggetti designati e autorizzati accedono alla Piattaforma ROC secondo modalità e logiche di elaborazione strettamente pertinenti e non eccedenti ai compiti attribuiti a ciascuno di essi.

In particolare, i MMG, avendo una conoscenza approfondita della storia clinica dei loro pazienti, delle loro condizioni e delle loro esigenze specifiche, svolgono un ruolo cruciale rappresentando il primo punto di contatto per i pazienti oncologici, identificando precocemente i sintomi sospetti e avviando tempestivamente i percorsi diagnostici e terapeutici.

La ROC - in virtù della sua struttura organizzativa avanzata, dell'approccio multidisciplinare al trattamento del cancro e all'implementazione di protocolli diagnostico-terapeutici condivisi - permette, attraverso il coinvolgimento di MMG,

migliorando la comunicazione e la collaborazione tra MMG e specialisti della ROC, di soddisfare le seguenti esigenze: assicurare che ogni paziente oncologico possa beneficiare delle migliori cure possibili, nel minor tempo possibile; implementare protocolli condivisi che facilitino un approccio integrato alla gestione del paziente oncologico; utilizzare strumenti tecnologici avanzati per la gestione dei dati clinici, rendendo il processo di cura più efficiente e coordinato; potenziare la collaborazione tra i vari attori del sistema sanitario per garantire ai pazienti oncologici un percorso di cura rapido, efficace e integrato.

1.6.1.4 SOGGETTI ESTERNI COINVOLTI NEL TRATTAMENTO

La **FONDAZIONE PASCALE** può **affidare a organizzazioni e collaboratori esterni, mediante atti idonei e conformi al GDPR,** attività o parti di attività inerenti alla ROC e alla Piattaforma; in particolare, può stipulare accordi contenenti i requisiti di cui all'art. 28 GDPR, demandando ad altre Organizzazioni (CRO, laboratori, Enti e Società di consulenza in genere) le attività che comportano il trattamento di dati personali riferiti ai singoli individui utenti della ROC e della Piattaforma.

In linea generale, nel rispetto di quanto prescritto dall'art. 28 Reg. UE 2016/679, i soggetti esterni che effettuino attività che possono comportare il trattamento dei dati relativi alla ROC devono essere designati Responsabili del trattamento in *outsourcing.*

Parimenti, i relativi contratti di consulenza, affidamento o manutenzione devono prevedere specifiche clausole di riservatezza dei dati, la registrazione degli interventi con l'indicazione degli orari di inizio e fine, le persone che li hanno effettuati e le motivazioni che hanno determinato la necessità dei medesimi interventi.

1.7 COMUNICAZIONE E DIFFUSIONE DEI DATI; TRASFERIMENTO EXTRA SEE

Ciascun Titolare del trattamento, per le sole finalità strettamente connesse al funzionamento della ROC, come indicate nel presente documento, può comunicare i dati oggetto di trattamento agli altri Titolari del trattamento previa osservanza di idonee

modalità tecniche di trasmissione dei dati medesimi in conformità alle misure di sicurezza vigenti, ai sensi della normativa in materia.

Tali modalità devono garantire un livello di sicurezza equivalente a quello assicurato dalle misure specificate nella presente VIP e nelle specifiche Policy inerenti alla ROC.

I dati personali dei pazienti registrati nella Piattaforma della ROC non saranno diffusi né pubblicati se non in forma aggregata e, quindi, in modo assolutamente anonimo, oppure secondo modalità che non rendano identificabili i soggetti interessati, per le sole finalità di cui alla presente DPIA.

I dati personali gestiti attraverso la Piattaforma web della ROC non saranno trasferiti verso Paesi Terzi rispetto all'Unione Europea o verso organizzazioni internazionali.

I Titolari non hanno intenzione di trasferire i dati personali a Paesi Terzi; in ogni caso, l'eventuale trasferimento dei dati verso Paesi extra SEE avverrà nel rispetto degli artt. 44 ss. GDPR (trasferimento sulla base di una decisione di adeguatezza e comunque soggetto a garanzie adeguate: clausole contrattuali tipo, ecc.).

1.8 TIPOLOGIA DI DATI TRATTATI

1.8.1 I dati personali oggetto di trattamento sono:

- dati personali comuni (nome, cognome, residenza, numero di telefono mobile, indirizzo e-mail, dati di contatto);
- categorie particolari di dati personali di cui all'art. 9 del GDPR ("dati sensibili": dati idonei a rivelare l'origine razziale ed etnica, dati relativi alla salute, dati genetici, dati relativi alla vita sessuale).

I dati personali relativi alla salute (in particolare, di carattere medico/clinico) delle persone registrate nella Piattaforma ROC vengono raccolti nell'ambito dell'attività clinica svolta dai professionisti sanitari specificamente autorizzati e, quindi, tramite visite mediche e accertamenti diagnostici o acquisiti dalle cartelle cliniche.

Nel database saranno raccolti e trattati, tra l'altro, i seguenti dati personali "sensibili": diagnosi e modalità di ammissione e dimissione, relative a prestazioni ambulatoriali

diagnostico terapeutiche; anamnesi; interventi chirurgici e procedure diagnostiche e terapeutiche; indagini cliniche e trattamenti eseguiti; in generale, informazioni relative a fattori prognostici, terapie farmacologiche, dati strumentali.

1.8.2 Fonti dei dati

I Titolari del trattamento relativo alla ROC effettuano la raccolta dei dati con le modalità e nel rispetto delle misure di sicurezza indicate nella presente VIP, attingendo, peraltro, agli archivi delle Aziende sanitarie, degli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) e delle strutture sanitarie private accreditate, limitatamente alle informazioni ivi contenute correlate alle patologie oncologiche, al fine di implementare la Piattaforma ROC con riferimento ai casi segnalati ed aggiornarla con l'inserimento di eventuali ulteriori casi.

Viene consultata, ove necessario, l'anagrafe degli assistiti per effettuare il raffronto dei dati anagrafici dei soggetti iscritti o da iscrivere nella Piattaforma con i dati anagrafici contenuti nella predetta Anagrafe, al fine di verificarne, ove necessario, l'esattezza e l'aggiornamento dei dati e individuare eventuali duplicazioni.

1.9 MODALITÀ DI TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali verrà effettuato, nel rispetto dei principi di correttezza, liceità e trasparenza, mediante l'utilizzo di strumenti manuali, informatici e telematici, strettamente correlati alle finalità sopra indicate.

I dati personali verranno trattati con modalità idonee a garantirne la sicurezza e la riservatezza in conformità alle disposizioni di cui all'art. 32 GDPR mediante l'adozione di misure, tecniche ed organizzative, idonee alla protezione dei diritti fondamentali degli Interessati.

Considerato che gli scopi della ricerca non possono essere compiutamente raggiunti mediante il trattamento di dati anonimi né senza l'identificazione, anche temporanea, degli Interessati, sono adottate, ove possibile e necessario, tecniche di cifratura e di pseudonimizzazione che rendano i dati personali trattati non direttamente riconducibili

agli Interessati, permettendo di identificarli solo in caso di necessità; in questi casi, i codici utilizzati non sono desumibili dai dati personali identificativi degli Interessati, salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato.

I dati raccolti e trattati vengono scelti ed individuati in relazione alle finalità secondo un criterio di congruità e nel rispetto della minimizzazione e sono conservati per un periodo non superiore alle finalità per le quali sono trattati.

Le finalità del trattamento sono individuate in modo chiaro e sintetico ed adeguatamente motivate negli atti di informativa.

Nessun dato personale trattato nell'ambito della Piattaforma ROC sarà soggetto a processo decisionale automatizzato e, in particolare, nessun dato trattato dai Titolari suindicati sarà soggetto ad attività di profilazione di cui all'articolo 22, paragrafi 1 e 4, del GDPR.

1.10 PRESUPPOSTI E FINALITÀ DELLA DPIA E RELATIVE RESPONSABILITÀ

La presente Valutazione d'Impatto sulla Protezione dei dati personali si rende necessaria ai sensi dell'art. 35 Reg. UE n. 2016/679 (GDPR) e dei Considerando 84, 89, 93, 95 ed alla luce delle Linee Guida WP 248 "in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento UE 2016/679" (in particolare, si applicano i criteri nn. 3, 4, 5, 7) nonché del Provvedimento del Garante per la protezione dei dati personali n. 467 dell'11/10/2018, "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, Reg. UE n. 2016/679" (in particolare, si applicano i criteri nn. 3, 6, 10).

I documenti sopra richiamati prescrivono che i titolari del trattamento sono tenuti ad effettuare valutazioni d'impatto sulla protezione dei dati se il trattamento riguarda dati sensibili o aventi carattere strettamente personale, dati inerenti a soggetti interessati vulnerabili e se si tratta di un trattamento a larga scala.

Nel caso di specie, il trattamento ha ad oggetto dati sensibili personali pseudonimizzati relativi a interessati vulnerabili (i pazienti oncologici registrati nella Piattaforma ROC) coinvolti nel trattamento sanitario e in eventuali progetti di ricerca.

E' opportuno evidenziare che, in linea generale, la **FONDAZIONE PASCALE**, indipendentemente dall'accertamento rigoroso della sussistenza delle condizioni sopra indicate che impongono la valutazione d'impatto, effettua le DPIA nel rispetto del principio di *accountability* e seguendo la specifica raccomandazione in tema di valutazione d'impatto delle Linee Guida WP 248, anche nei casi in cui non risulti certa l'obbligatorietà delle stesse, ritenendo che la VIP sia "uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati"; (Linee Guida WP 248).

Nel caso in esame, il trattamento dei dati personali relativi alla salute e la funzionalità della Piattaforma ROC rispetto alle esigenze di prevenzione, diagnosi e cura nonché all'attività di ricerca scientifica determinano, in prima analisi, livelli elevati di verosimiglianza e di impatto sicchè deve ritenersi sussistente il criterio dell' "alto rischio" di cui all'art. 35 GDPR.

La redazione del presente documento ha tenuto conto, in particolare, delle normative, provvedimenti e documenti di seguito elencati, ancorché in modo non esaustivo:

- **Reg. UE 2016/679**: artt. 5, 6, 9, 12, 13, 14, 24, 25, 32, 33 34, 35, 89
- **D.Lgs. 196/03** - **CODICE PRIVACY**: artt. 110 e 110 bis, comma 4;
- **EDPS (European Data Protection Supervisor)**
  - *A Preliminary opinion on data protection and scientific reserach* - 6/01/2020;
- **EDPB (European Data Protection Board)**
  - *Parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati* (articolo 70, paragrafo 1, lettera b)).
  - *Guidelines 3/2020 on the processing of data concerning health for the purpose of scientific research in the context of the Covid-19 outbreak* - 21/04/2020;

- *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, del 2/2/2021;

- **Garante per la protezione dei dati personali**:

- Provvedimento n. 146 del 5/06/2019 recante le prescrizioni relative al trattamento di categorie particolari di dati, ex art. 21, comma 1, D.Lgs. n. 101/18 e, in particolare: Prescrizioni relative al trattamento dei dati genetici e Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (All. 4 e 5 del Provvedimento 5/06/2019);

- Provvedimento n. 55 del 7/03/2019 in merito all'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario;

- Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica (All. A5 al Codice Privacy) e successivo Provvedimento 9/05/2024 sulle garanzie da applicare ai sensi del riformato art. 110 del Codice Privacy

- Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali del 24/07/2008;

- Presupposti giuridici e principali adempimenti per il trattamento da parte degli IRCCS dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca e relative FAQ.

La redazione del presente documento ha tenuto conto, inoltre, del fatto che si può ricorrere a una singola valutazione d'impatto sulla protezione dei dati nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi.

Invero, ai sensi dell'art. 35 GDPR e delle citate **Linee Guida WP 248** in materia di valutazione d'impatto sulla protezione dei dati, una **DPIA può esaminare un singolo trattamento o un insieme di trattamenti simili** (art. 35, paragrafo 1: "una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi"; Considerando 92: "vi sono circostanze in cui può essere ragionevole ed

economico effettuare una **valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni** o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata".

Infine, si evince dal contesto normativo e regolatorio e, in particolare, dalle **Linee Guida WP 248** che una VIP può essere utile per valutare **l'impatto sulla protezione dei dati di un prodotto tecnologico, ad esempio un dispositivo hardware o un software, qualora sia probabile che lo stesso venga utilizzato da titolari del trattamento distinti per svolgere tipologie diverse di trattamento**: "Ovviamente, il titolare del trattamento che utilizza detto prodotto resta soggetto all'obbligo di svolgere la propria valutazione d'impatto sulla protezione dei dati in relazione all'attuazione specifica; tuttavia, nell'ambito di tale valutazione, i diversi titolari del trattamento possono utilizzare le informazioni fornite da una valutazione analoga preparata dal fornitore del prodotto, se opportuno".

Nel caso in esame, la relazione intercorrente tra i vari titolari del trattamento aderenti alla ROC determina le condizioni per la predisposizione della presente DPIA.

1.11 CRITERI, METODI E STANDARD DI RIFERIMENTO UTILIZZATI PER LA REDAZIONE DELLA VIP.

Il presente documento è stato predisposto per individuare potenziali lacune nel sistema di gestione attuale della ROC e della relativa Piattaforma e pianificare interventi e soluzioni delle lacune individuate

Pertanto, può e deve essere utilizzato come riferimento per determinare e implementare i controlli per il trattamento del rischio relativo alla sicurezza dei dati personali inerenti alla ROC, attraverso un microsistema di gestione della sicurezza delle informazioni di questo specifico trattamento riconducibile alla FONDAZIONE PASCALE.

La protezione dei dati personali oggetto del trattamento in esame è implementata mediante un insieme adeguato di controlli (politiche, regole, processi, procedure, strutture organizzative, funzioni software e hardware) volti a conseguire gli obiettivi di sicurezza strettamente correlati alla natura e agli scopi della ROC, definendo, implementando, monitorando, riesaminando e migliorando questi controlli ove necessario.

Per la redazione della VIP si è tenuto conto di tre aspetti rilevanti:

- la valutazione dei rischi cui sono esposti gli Interessati, effettuata tenendo conto della natura e degli scopi della ROC, supportata da preventive attività di identificazione e analisi dei rischi relativi alla sicurezza delle informazioni con determinazione dei controlli necessari per assicurare che il rischio residuo per l'organizzazione soddisfi i criteri di accettazione del rischio;

- i requisiti legali, regolamentari e contrattuali che la FONDAZIONE PASCALE e le altre parti interessate (Centri partecipanti alla ROC, fornitori di servizi, ecc.) dovrebbero rispettare;

c) i principi, gli obiettivi e i requisiti relativi a tutte le fasi del ciclo di vita delle informazioni che la FONDAZIONE PASCALE ha sviluppato a supporto delle proprie operazioni.

Questo documento costituisce la valutazione d'impatto sulla protezione dei dati relativa alla ROC e alla sua Piattaforma ma, al contempo, può essere considerato un punto di partenza per lo sviluppo di linee guida e procedure specifiche dell' IRCSS PASCALE e delle altre Organizzazioni coinvolte nella ROC.

Non tutti i controlli e le misure previsti in questo documento possono essere applicabili a tutte le Organizzazioni coinvolte nella ROC e ulteriori controlli, procedure e misure non inclusi nel presente documento possono essere adottati per far fronte alle esigenze specifiche delle singole Organizzazione e ai rischi che sono stati identificati. Qualora venissero predisposti documenti contenenti procedure, controlli e misure aggiuntivi, sarebbe utile includere riferimenti incrociati ai paragrafi di questo documento per

applicazioni e riferimenti futuri.

Il presente documento è stato predisposto tenendo conto dei seguenti standard, documenti e linee guida:

- Schema di implementazione del CNIL;
- ENISA - Linee Guida e Manuale sulla sicurezza nel trattamento dei dati personali;
- Standard ISO/IEC e Linee guida: 31000, 27005, 27001 e 27002;
- Linee guida EDPB 4/2019 sull'art. 25 GDPR;
- Misure minime di sicurezza ICT per le p.a. MMAgID;
- Linee Guida OSWAP.

1.12 RISORSE DI SUPPORTO DEI DATI PERSONALI.

Le risorse cui sono imputabili i dati personali oggetto di trattamento sono le seguenti:

- Piattaforma ROC;
- Cartelle cliniche e documenti sanitari dei pazienti in possesso dei professionisti e Centri aderenti alla ROC e presenti su dispositivi informatici e supporti cartacei;
- Server mail per la comunicazione criptata delle informazioni.

2. PRINCIPI FONDAMENTALI E MISURE - NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO - TUTELARE DEI DIRITTI DEGLI INTERESSATI

2.1 NECESSITÀ E PROPORZIONALITÀ DEI TRATTAMENTI IN RELAZIONE ALLE FINALITÀ E ALLE BASI GIURIDICHE (art. 35, par. 7, lett. b) reg. ue 2016/679)

2.1.1 LE FINALITÀ DEL TRATTAMENTO

I dati personali saranno trattati, nell'ambito dei servizi erogati in favore degli Interessati, previo inserimento nella Piattaforma web della ROC, tenendo conto del citato Decreto n. 98/2016.

La ROC, come già rilevato, nasceva dall'esigenza di migliorare la gestione dei pazienti oncologici nella Regione Campania, creando un sistema informativo condiviso che permettesse la comunicazione in tempo reale tra i vari nodi della rete.

Ciò premesso, le finalità della ROC e della relativa Piattaforma web sono:

- definizione del miglior approccio terapeutico da adottare per la prevenzione, diagnosi, cura dei tumori maligni e riabilitazione;
- presa in carico dell'Interessato presso uno dei Centri terapeutici abilitati ad erogare le prestazioni diagnostiche e terapeutiche oncologiche;
- integrazione dei servizi sanitari e sociali per l'assistenza oncologica, coordinando le professionalità e le istituzioni coinvolte nella prevenzione, diagnosi, terapia e riabilitazione oncologica;
- valutazione della corretta applicazione dei Percorsi Diagnostico Terapeutici (PDTA) e della performance della ROC;
- pianificazione dei servizi sanitari da erogare, controllo e valutazione dei servizi erogati.

In definitiva, gli scopi principali della ROC e della sua Piattaforma sono:

- ottimizzare la presa in carico e i percorsi di cura dei pazienti nella gestione delle patologie neoplastiche,
- garantire la continuità di cura con un rapido invio delle richieste verso le strutture

sanitarie preposte per i servizi domiciliari territoriali.

Ulteriori obiettivi della Piattaforma, strettamente correlati agli scopi sopra indicati e funzionali al raggiungimento degli stessi, sono:

consentire a tutti i Centri che ne fanno parte, per i rispettivi ambiti di competenza, di contribuire all'attuazione di percorsi assistenziali, organizzati ed efficienti;

assicurare una gestione multidisciplinare integrata;

garantire il rispetto dei principi di appropriatezza ed equità di accesso alle cure;

rafforzare l'empowerment e il ruolo proattivo dei MMG nella rete di presa in carico affrontando le barriere incontrate nella pratica clinica;

strutturare e coordinare le attività della ROC, GOM e PDTA evidenziando i vantaggi del percorso del paziente nella Rete;

favorire il network costruttivo tra tutti gli attori coinvolti nel percorso di cura del paziente oncologico.

2.1.2 BASI GIURIDICHE PER IL TRATTAMENTO DEI DATI

Le basi giuridiche del trattamento vengono individuate in base al contesto normativo e regolatorio vigente.

La **FONDAZIONE PASCALE**, in quanto IRCCS, è un Ente del Servizio sanitario nazionale che persegue, secondo standard di eccellenza, finalità di ricerca, soprattutto clinica e traslazionale, nel campo biomedico e in quello dell'organizzazione e gestione dei servizi sanitari e garantisce prestazioni di ricovero e cura di alta specialità (art.1 d.lgs. 16/10/2003, n. 288).

La **FONDAZIONE PASCALE** fonda la legittimità delle attività di trattamento dei dati personali relativi alla ROC su specifiche condizioni di liceità.

Di seguito verranno elencate e descritte le singole attività di trattamento con le relative finalità correlate alle rispettive “basi giuridiche” o “condizioni di liceità”.

2.1.3 BASE GIURIDICA PER IL TRATTAMENTO DEI DATI A FINI DIVERSI DALLA RICERCA SCIENTIFICA:

- **le attività necessarie per la prevenzione, cura, diagnosi, riabilitazione e assistenza o terapia sanitaria o sociale** in base al diritto europeo o nazionale o in conformità al contratto con un professionista della sanità sono fondate sulla seguente base giuridica: finalità di cura ai sensi degli artt. 6, par 1, lett. e) e 9, par 2, lett. h) GDPR;

- le attività **amministrative** strettamente connesse al raggiungimento delle finalità di prevenzione, cura, diagnosi, riabilitazione e assistenza o terapia sanitaria o sociale, lo **svolgimento di compiti** del S.S.N. e dei soggetti operanti in ambito sanitario, di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, tutela della vita e incolumità fisica e le **attività con fini di programmazione**, gestione, controllo e valutazione dell'assistenza sanitaria sono fondate sulla seguente base giuridica: perseguimento di un interesse pubblico rilevante ai sensi degli artt. 6, par. 1, lett. e) e 9, par. 2, lett. g) del GDPR e dell'art.2-sexies del Codice Privacy

- le attività connesse a 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 sono fondate sulla base giuridica di cui all'art. 9, par. 2, lett. i) GDPR;

- le attività di consultazione, conservazione, archiviazione e condivisione tra diversi Titolari dei dati personali (successive all'accesso ai servizi della Piattaforma web della ROC) volontariamente forniti e/o acquisiti durante le prestazioni diagnostiche e terapeutiche, sono fondate sulla base giuridica del consenso esplicito dell'interessato; dunque, per le **funzionalità legate all'utilizzo della Piattaforma** (consultazione, conservazione, archiviazione e condivisione delle informazioni inserite) correlate alle "finalità di cura", la base legale del trattamento è il consenso esplicito dell'interessato, ai sensi degli artt. 6, par. 1, lett. a) e 9, par. 2, lett. a) GDPR; in ogni caso, qualora i pazienti non fornissero il consenso al trattamento dei dati funzionale all'utilizzo della Piattaforma, ciò non precluderebbe l'erogazione delle prestazioni sanitarie che

verrebbero comunque fornite e l'unica conseguenza sarebbe l'impossibilità di attivare le funzionalità garantite dalla Piattaforma web della ROC, sotto il profilo dell'ottimizzazione delle attività di presa in carico e dei percorsi di cura; tale circostanza è evidenziata e illustrata nell'atto di informativa/consenso sottoposto ai pazienti prima di procedere alla registrazione dei loro dati in Piattaforma.

2.1.4 BASE GIURIDICA PER IL TRATTAMENTO DEI DATI A FINI DI RICERCA SCIENTIFICA

2.1.4.1 La FONDAZIONE PASCALE, per poter utilizzare i dati dei suoi pazienti anche per l'attività di ricerca scientifica, deve individuare sia le basi giuridiche idonee a legittimare tale trattamento sia una deroga adeguata al generale divieto di trattare i dati sulla salute e genetici.

Ciò premesso, la FONDAZIONE PASCALE, con specifico riferimento al trattamento dei dati raccolti e registrati nell'ambito della **ROC e della relativa Piattaforma**, può individuare la **base di liceità del trattamento** dei dati personali raccolti a scopo di cura per ulteriori finalità di ricerca, oltre che sul **consenso** dei partecipanti alla ricerca, sull' **art. 110-bis, comma 4 del Codice privacy**, secondo il quale non costituisce trattamento ulteriore dei dati raccolti per l'attività clinica, quello svolto a fini di ricerca.

Pertanto, la FONDAZIONE PASCALE fonda il trattamento dei dati relativi alla ROC e alla relativa Piattaforma, con riferimento alla ricerca scientifica, sul consenso degli interessati, ai sensi degli artt. 6, par. 1, lett. a) e 9, par. 2, lett. a) del Regolamento, differenziando tale manifestazione di volontà inerente alla protezione dei dati dal c.d. consenso informato all'adesione volontaria alla ricerca da parte degli interessati, previsto dalla specifica disciplina di settore e dai pertinenti standard etici.

Qualora la FONDAZIONE PASCALE dovesse avvalersi, in qualità di IRCCS, del citato art. 110-bis, comma 4, Codice privacy svolgerà la relativa VIP (Valutazione d'impatto), pubblicandola sul proprio sito web, in una sezione agevolmente accessibile agli utenti, per l'intera durata dello Studio, osservando le modalità per informare i partecipanti alla ricerca a seconda che i dati siano raccolti presso la FONDAZIONE ovvero presso banche dati interne all'Istituto o altri centri partecipanti.

Nel caso in cui i dati siano raccolti direttamente presso gli interessati, l'IRCCS PASCALE fornisce preventivamente e direttamente in una forma chiara, concisa ed intellegibile, le informazioni, ai sensi dell'art. 13, par. 3 del Regolamento, eventualmente limitandosi ad evidenziare quegli elementi informativi **di cui** l'interessato non dispone già**,** ai sensi dell'art. 13, par. 4 del Regolamento.

Nelle ipotesi in cui i dati siano raccolti presso banche dati interne dell'Istituto ovvero presso terzi, le informazioni possono essere rese secondo le modalità di cui all'art. 14, par. 5, lett. b) del Regolamento che ne ammette la pubblicazione; allo stato le Regole deontologiche, ribadite e integrate nel Provvedimento del Garante privacy 9/5/2024, forniscono delle indicazioni su come pubblicare tali informazioni (cfr. art. 6, comma 3).

Conformemente a tale provvedimento, il Garante privacy ha segnalato come efficaci modalità per rendere note le informazioni ai sensi dell'art. 14, par. 5, lett. b) del Regolamento e dell'art. 6, comma 3 delle Regole deontologiche, la pubblicazione sul sito web del Promotore e, nel caso di studi multicentrici, anche sui siti web dei centri partecipanti, per tutta la durata dello studio.

Per i pazienti deceduti o non contattabili, nell'ambito della raccolta retrospettiva dei dati personali, la base di liceità del trattamento viene individuata, ai sensi degli 'artt. 110 e 110 bis, comma 4, Codice Privacy e dell'art. 9, par. 2, lett. j) del Regolamento, nella pubblicazione della VIP e dell'informativa ex art. 14, par. 5, lett. b) Reg. UE 2016/679 e 6, comma 3 Regole deontologiche, nella relativa comunicazione al Garante Privacy, tenendo conto delle indicazioni di cui al provvedimento del Garante Privacy del 9/05/2024 n. 298.

2.1.4.2 Con specificor riferimento alla base giuridica del consenso e tenendo conto del contesto normativo e regolatorio, l'Istituto Nazionale Tumori IRCCS "Fondazione G.Pascale" – volendo contemperare la ricerca e il suo progredire con i diritti degli interessati attuando il principio di trasparenza – intende avvalendosi del c.d. "consenso a fasi progressive".

La **FONDAZIONE PASCALE** acquisirà, pertanto, un consenso espresso relativo allo Studio Oncocamp nonchè un consenso all'analisi generica dei dati contenuti nella

Piattaforma/data base al fine di poter individuare ricerche specifiche e poter procedere, in un secondo momento, all'ottenimento di consensi specifici e dettagliati per ogni singolo Protocollo o Progetto di ricerca.

Questa prospettiva:

- appare favorevole per lo sviluppo delle attività di ricerca, in quanto la possibilità garantita ai ricercatori di consultare i dati contenuti nel database/piattaforma ROC costituisce il presupposto necessario per comprendere quali ricerche potrebbero nascere dal citato database;
- risulta avallata e incoraggiata dal Garante Privacy favorevole alla distinzione del trattamento in due diverse fasi (Cfr., tra gli altri, Garante Privacy, Parere 50 del 30 giugno 2022):

a) creazione del database, con corretta individuazione delle basi giuridiche nel consenso o negli artt. 110 e 110 bis Codice Privacy;

b) possibile svolgimento di nuove ricerche sui dati raccolti.

La FONDAZIONE PASCALE posto che, allo stato, non è possibile individuare pienamente le specifiche finalità di ricerca scientifica e che, al momento della raccolta del consenso per l'inclusione dei pazienti nella Piattaforma, le future attività di ricerca non saranno ancora state definite se non in termini generali, provvede, quale Titolare e Promotore, ad ottenere un consenso ogniqualvolta verrà sviluppato un nuovo Progetto di ricerca, conseguendo, dunque, un consenso "a fasi progressive".

In definitiva, la **FONDAZIONE PASCALE**, una volta acquisita l'approvazione dei Comitati Etici, dovrà integrare le manifestazioni di volontà degli Interessati con specifici consensi fino a giungere, in via progressiva, ad ottenere un presupposto giuridico idoneo al trattamento dei dati per scopi di ricerca scientifica.

Dunque, i dati all'interno della Piattaforma ROC vengono raccolti con un consenso specifico e il consenso alla creazione della banca dati consentirà lo svolgimento dell'attività di ricerca in via generale, consistente nella definizione di quelli che saranno i futuri Progetti di ricerca, essendo la banca dati destinata ad essere rappresentata

pienamente proprio nei futuri Progetti di ricerca.
In altri termini, i Progetti originariamente individuati al momento della costituzione della Piattaforma sono assimilabili alle stesse finalità del trattamento della banca dati ma non ai Progetti effettivi che potranno essere presentati a un comitato etico.

2.2 NECESSITÀ E PROPORZIONALITÀ DEI TRATTAMENTI (art. 35, par. 7, lett. b) Reg. UE 2016/679) – MISURE VOLTE ALLA TUTELA DEI DIRITTI DEGLI INTERESSATI.

2.2.1 Il trattamento è conforme ai principi di liceità, correttezza e trasparenza.

Ricorrono, nel caso di specie, le basi di liceità del trattamento indicate nella presente VIP e i dati sono trattati in osservanza dei principi di correttezza e trasparenza, attraverso adeguati atti di informativa e consenso nonché mediante le nomine dei Responsabili del trattamento ai sensi dell'art. 28 GDPR e degli autorizzati e designati al trattamento ai sensi degli artt. 29 GDPR e 2-quaterdecies D.Lgs. 196/03; (EDPB - Linee Guida 1/2022 sui diritti degli interessati; EDPB - Linee guida 5/2020 sul consenso).
I Titolari si impegnano a conferire l'informativa agli Interessati anche dopo la raccolta nei casi in cui ciò sia possibile e ove questi si rivolgano ai Centri partecipanti, anche per visite di controllo, anche al fine di consentire loro di esercitare i diritti previsti dalla normativa vigente.
Con riferimento alla ricerca scientifica l'inizio dei trattamenti dei dati personali necessari per la realizzazione degli Studi è condizionato all'ottenimento dei definitivi pareri favorevoli dei competenti comitati etici, così integrando le specifiche condizioni di liceità del trattamento dei dati personali già richiamate (Cfr. Provv. n. 202 del 29/10/2020, doc. web 951741; n. 406 del 1/11/2021, doc. web 9731827; n. 73 del 2/03/2023, doc. web 9875254).

2.2.2 Gli scopi del trattamento sono specifici, espliciti e legittimi.

Gli scopi del trattamento dei dati sono considerati specifici, espliciti e legittimi per diverse ragioni:

a) il trattamento dei dati effettuato nell'ambito della Piattaforma è orientato a raggiungere le finalità determinate e legittime e gli specifici obiettivi della ROC, individuati nel contesto normativo e regolatorio vigente;
b) i dati saranno trattati esclusivamente per le finalità della ROC per la realizzazione delle quali essi saranno raccolti e inseriti nel data-base.

2.2.3 I dati sono esatti e aggiornati

I dati raccolti nella Piattaforma sono conformi e verificati per garantire la loro accuratezza e aggiornamento.

Tutti gli utenti della Piattaforma si impegnano a seguire procedure per la raccolta e verifica dei dati, effettuando le verifiche utili a garantire l'attendibilità e l'accuratezza delle informazioni raccolte.

Sono adottate misure ragionevoli per la rettifica o cancellazione dei dati inesatti.

I Titolari del trattamento e gli altri soggetti coinvolti nella Piattaforma prestano particolare attenzione alla formazione del personale, soprattutto con riferimento alle fasi in cui i dati vengono caricati e raccolti dai soggetti di riferimento, ciò al fine di presidiare e mitigare adeguatamente il rischio dell'errore umano; in tal senso, tutti gli utenti si impegnano a fornire specifiche istruzioni scritte.

In definitiva, per garantire l'effettiva applicazione del principio di esattezza dei dati sono predisposte le seguenti misure tecniche ed organizzative:

- gli utenti prestano la massima attenzione nelle operazioni di *data entry* nella Piattaforma e tali operazioni non sono affidate a personale amministrativo;
- i dati non verranno utilizzati senza assicurarsi che essi siano accurati ed aggiornati;
- i dati inesatti rispetto alle finalità del trattamento per le quali sono stati raccolti vengono modificati o rettificati tempestivamente senza ritardi;

- viene eseguito il monitoraggio dei dati raccolti per tutto il ciclo vitale.

Pertanto, le misure, preventive e successive, adottate per limitare il più possibile la possibilità di errore, comprendono: la validazione dei dati, la verifica di coerenza dei dati inseriti; la segnalazione di eventuali errori o problematiche nella raccolta; il rifiuto di raccolta di dati incompleti o imprecisi.

2.2.4 Come sono informati del trattamento gli interessati.

Verrà raccolto il consenso informato degli Interessati alla partecipazione alla Piattaforma e al trattamento dei dati personali inerenti alla ROC in tutti i casi in cui sarà possibile fornire loro un'adeguata informazione e quindi acquisirne il relativo consenso.

Dunque, i Centri partecipanti inviteranno gli Interessati, mediante plurimi e idonei sistemi di comunicazione, a mettersi in contatto con le strutture ospedaliere competenti in modo da fornire loro ulteriori informazioni; l'obiettivo di tale modalità di comunicazione è quello di garantire che tutte le persone interessate abbiano accesso alle informazioni pertinenti relative alla ROC e alla Piattaforma ed abbiano la possibilità di prendere una decisione consapevole e informata sulla partecipazione.

2.2.5 Come si ottiene il consenso degli interessati.

I Centri partecipanti, che hanno il compito di arruolare i pazienti alla Piattaforma, dovranno preventivamente ottenere da ciascun paziente la sottoscrizione del documento di consenso informato scritto.

Dunque, i Centri partecipanti, si impegnano, tramite i professionisti sanitari appositamente autorizzati, a rendere l'informativa agli interessati inclusi nella Piattaforma al fine di acquisirne il consenso informato relativo al trattamento dei dati personali.

2.2.6 Il trattamento è conforme al principio di "necessità".

La mancata raccolta dei dati personali nella Piattaforma potrebbe non garantire il conseguimento delle finalità principali e secondarie della ROC che potrebbero non essere

raggiunte attraverso modalità alternative che incidano meno sui diritti e sulle libertà degli Interessati.

Il perseguimento delle finalità della Piattaforma presuppone la raccolta ed il trattamento di dati, con le modalità descritte nel presente documento al fine di realizzare dette finalità.

2.2.7 Il trattamento è conforme al principio di "limitazione della finalità".

I dati sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo compatibile con tali finalità.

Le finalità sono riconducibili alla disciplina, normativa e regolamentare, nazionale e regionale, e agli obiettivi di assistenza, cura e ricerca scientifica suindicati e descritti.

2.2.8 Il trattamento è conforme al principio di "minimizzazione dei dati".

Sono raccolti e trattati soltanto i dati personali necessari al raggiungimento delle finalità della ROC.

Tutte le misure, tecniche ed organizzative, sono volte alla minimizzazione dei dati.

Dunque, in applicazione del principio di minimizzazione:

a) la Piattaforma **ROC** e i sistemi informativi sono configurati riducendo al minimo l'utilizzazione dei dati personali, escludendone il trattamento quando le finalità perseguite possono realizzarsi con modalità che permettono di identificare gli Interessati solo in caso di necessità;

b) il trattamento di dati personali per gli scopi di cura e ricerca riguarda i dati relativi alla salute degli interessati e, solo ove indispensabili per il raggiungimento delle finalità della ricerca, anche i dati relativi all'origine razziale ed etnica;

c) i dati saranno trattati soltanto dai soggetti formalmente coinvolti nelle operazioni di trattamento e specificamente autorizzati al trattamento e non saranno in alcun modo comunicati a soggetti esterni o diffusi.

2.2.9 Il trattamento è conforme al principio di "proporzionalità".

Il trattamento riguarda dati personali rilevanti, completi e non eccessivi in relazione agli scopi per i quali sono raccolti e successivamente trattati nonché adeguati e pertinenti ai fini del trattamento.

Il trattamento dei dati è proporzionale e meritevole di considerazione in ragione del contesto, della natura e delle finalità del trattamento.

La ROC e la relativa Piattaforma sono caratterizzati da una notevole utilità clinica e scientifica ed il relativo trattamento comporta rischi, rispetto ai dati personali ed ai diritti ed alle libertà degli Interessati, ritenuti "mitigabili" e, dunque, "accettabili" in ragione dei motivi esposti nella presente DPIA e dell'adozione delle misure ivi elencate e descritte.

2.2.10 Individuazione dei rischi per i diritti e le libertà degli interessati (art. 35, par. 7, lett. c) Reg. UE 2016/679).

I rischi per i diritti e le libertà delle persone fisiche interessate, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale.

La probabilità e la gravità del rischio per i diritti e le libertà degli Interessati sono state accertate in base a una valutazione oggettiva, con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento.

2.3 Misure previste per affrontare e mitigare i rischi (art. 35, par. 7, lett. d) Reg. UE 2016/679).

L'implementazione, gestione e tenuta della Piattaforma comporta il trattamento di dati personali e, in particolare, l'attuazione di operazioni di raccolta, registrazione e conservazione dei dati dei pazienti registrati.

Pertanto, sono adottate misure, tecniche ed organizzative idonee alla protezione dei dati personali per garantire la riservatezza, l'integrità e la disponibilità dei dati raccolti e registrati.

Sono adottate, inoltre, misure di sicurezza proporzionate ai rischi per i diritti e le libertà delle persone fisiche derivanti dai casi di distruzione accidentale o illecita, perdita, alterazione,

divulgazione non autorizzata o accesso ai dati personali trattati nonché implementate strutture interne e politiche in grado di assicurare l'attuazione di tali misure di sicurezza, sia al momento di definire i mezzi di trattamento sia all'atto del trattamento stesso (compresa l'esecuzione della presente VIP).
Dette misure di sicurezza permettono agli Interessati di esercitare i propri diritti ai sensi degli artt. 15-22 del GDPR.

2.3.1 Come fanno gli interessati a esercitare i loro diritti di accesso, portabilità e limitazione dei dati.

Nel foglio informativo e modello di consenso al trattamento predisposto dall' **IRCCS PASCALE** fornito ai Centri Partecipanti è chiaramente indicato che gli Interessati hanno il diritto di esercitare i loro diritti e che per fare ciò possono rivolgersi direttamente al Centro clinico di riferimento.
All'interno del Centro clinico, gli Interessati possono contattare il Referente privacy del trattamento dei dati o la persona autorizzata al trattamento dei dati personali, che operano sotto l'autorità diretta del Titolare. Queste figure sono specificamente designate per gestire le richieste degli Interessati e fornire assistenza per l'esercizio dei loro diritti.
Attraverso questa modalità, gli Interessati hanno la possibilità di richiedere informazioni sui dati personali che sono stati raccolti nel contesto della ROC e di esercitare i propri diritti se lo desiderano.

2.3.2 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione

Qualora siano necessarie modifiche ai dati personali, verranno appositamente annotate le modifiche richieste dall'Interessato.
Questa pratica viene adottata al fine di garantire l'integrità e la tracciabilità dei dati originalmente immessi in Piattaforma.
L'annotazione delle modifiche richieste dall'Interessato senza alterare i dati originariamente immessi in Piattaforma, consente di mantenere un registro accurato delle richieste e delle

eventuali modifiche apportate, garantendo al contempo la coerenza e l'integrità delle informazioni conservate.

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

Per la realizzazione della ROC e della Piattaforma la **FONDAZIONE PASCALE** può avvalersi del supporto di responsabili esterni (selezionati con attenzione) i quali si obbligheranno a rispettare rigorosi obblighi di sicurezza e riservatezza dei dati personali.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto regolarmente sottoscritto.

Il contratto sottoscritto con i responsabili del trattamento stabilisce, in modo chiaro, i compiti e le responsabilità di ciascuna parte coinvolta; vengono definiti i limiti e le finalità del trattamento dei dati personali nonché le misure di sicurezza che devono essere implementate per proteggere tali dati.

Questo contratto fornisce una base legale solida per regolare la relazione tra i titolari del trattamento e i responsabili esterni, garantendo che ogni parte sia consapevole dei propri obblighi e delle modalità di trattamento dei dati personali.

2.4 Misure di sicurezza inerenti al trattamento dei dati relativi alla ROC e alla sua Piattaforma

2.4.1 Disposizioni generali

La sicurezza dei dati contenuti nella Piattaforma deve essere garantita **in tutte le fasi del trattamento**, adottando opportuni accorgimenti che preservino i medesimi dati da rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato, modifiche indesiderate o di trattamento non consentito o non conforme alle finalità della raccolta.

La **FONDAZIONE PASCALE** (Titolare del trattamento in quanto Corpus e Responsabile in merito alla realizzazione, gestione e tenuta della Piattaforma) e i Centri e le Strutture presso

le quali sono raccolti i dati che alimentano la ROC e la Piattaforma (Titolari autonomi e Organizzazioni deputate a comunicare o mettere a disposizione i dati nella Piattaforma ROC) devono adottare:

- **quantomeno, le seguenti misure di sicurezza:**

a) sistemi antivirus e antimalware costantemente aggiornati;

b) sistemi di protezione perimetrale, costantemente attivati e adeguatamente configurati in funzione del contesto operativo (firewall);

c) software di base e applicativi costantemente aggiornati.

- in particolare, le seguenti ulteriori misure:

- misure idonee a garantire la qualità dei dati e la corretta attribuzione agli Interessati;

- misure idonee a garantire la protezione dei dati dai rischi di accesso abusivo ai dati o modifiche indesiderate degli stessi (mediante applicazione di tecnologie crittografiche a *file system* o *database* e adozione di altre misure che rendano inintelligibili i dati ai soggetti non legittimati nelle operazioni di registrazione e archiviazione dei dati);

- canali di trasmissione protetti, basati sull'utilizzo di *standard* crittografici per la trasmissione elettronica dei dati raccolti, per la comunicazione dei dati raccolti nell'ambito della Piattaforma (dove sono memorizzati e archiviati) e eventuali organizzazioni e soggetti esterni di cui lo stesso Titolare/Promotore si avvale;

- tecniche di conservazione e trasmissione dei dati, mediante codici identificativi ed analoghe soluzioni che li rendono non direttamente riconducibili agli Interessati, permettendo di identificare questi ultimi solo in caso di necessità.

Dette misure di sicurezza sono predisposte, attuate e verificate durante lo svolgimento dell'intero trattamento:

- nella fase di raccolta, memorizzazione e archiviazione dei dati;

- nella fase successiva di elaborazione dei dati stessi;

- nella fase di conservazione e cancellazione.

2.4.2 Fase di raccolta, memorizzazione e archiviazione dei dati

La **raccolta dei dati** dovrà conformarsi a quanto prescritto nelle **Procedure relative all'IRCCS Pascale** e, in ogni caso, alle seguenti prescrizioni e modalità:

a) garantire l'accesso selettivo ai soli dati oggetto della Piattaforma;
b) assegnare al personale autorizzato al trattamento credenziali di autenticazione e profili di autorizzazione specifici alle attività di consultazione e raffronto;
c) predisporre strumenti e procedure per il meccanismo di autorizzazione e autenticazione del personale incaricato al trattamento dei dati nonché per delimitare nel tempo e nella localizzazione, la possibilità di accesso ai medesimi dati garantendo che:

   la raccolta dei dati avvenga soltanto tramite l'uso di postazioni di lavoro appartenenti alla rete IP dei Centri partecipanti;

   la password venga consegnata al singolo autorizzato separatamente rispetto al codice per l'identificazione e sia modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni sei mesi;

   siano preferibilmente utilizzati sistemi di autenticazione a più fattori per l'abilitazione degli autorizzati e per l'accesso telematico alla Piattaforma;

   sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;

   sia vietato l'utilizzo di dispositivi automatici che consentano di consultare i dati in forma massiva;

   siano disattivate le credenziali di autenticazione non utilizzate da almeno sei mesi.

d) effettuare periodiche verifiche, anche a fronte di cambiamenti organizzativi o eventi anomali, circa la sussistenza dei presupposti che hanno originato l'abilitazione degli autorizzati; eventuali esiti negativi delle predette verifiche devono dar luogo alla tempestiva revisione del profilo di abilitazione, alla eventuale disabilitazione dello stesso o alla disattivazione delle credenziali;
e) prevedere la registrazione in appositi file di log, ai fini della verifica della correttezza e legittimità del trattamento dei dati, delle seguenti informazioni: il soggetto (codice identificativo) che ha effettuato l'accesso, la data e l'ora dell'accesso, l'operazione

effettuata, l'indirizzo IP della postazione di accesso e del server interconnesso, i dati trattati.

Inoltre:

- i log sono protetti con idonee misure contro ogni uso improprio;
- i log sono conservati, di regola, per 24 mesi e cancellati alla scadenza;
- i dati contenuti nei log sono trattati da personale appositamente autorizzato al trattamento esclusivamente in forma aggregata; possono essere trattati in forma non aggregata unicamente laddove ciò risulti indispensabile ai fini della verifica della correttezza e legittimità delle singole operazioni effettuate;

f) utilizzare sistemi di audit log per la verifica periodica degli accessi ai dati e per il rilevamento delle anomalie.

Le modalità tecniche di raccolta dei dati sono le seguenti:

- accesso diretto degli autorizzati ai sistemi informatici delle strutture sanitarie (raccolta dei dati in capo ai medici che operano presso le strutture) e successivo caricamento degli stessi nella Piattaforma;

- in casi eccezionali e residuali: trasmissione/acquisizione di documenti cartacei in plico chiuso e sigillato;

Più precisamente, i Titolari del trattamento inerente alla ROC e alla relativa Piattaforma **istruiscono gli autorizzati**, individuati ai sensi della normativa vigente in materia di protezione dei dati personali, sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina in materia di protezione dei dati personali più rilevanti in rapporto alle relative attività, nonché sulle responsabilità che ne derivano.

Ove si verifichi un caso eccezionale e residuale, connotato da urgenza ed indifferibilità, che impone il trattamento analogico/cartaceo dei dati personali, i Titolari del trattamento dei dati relativi alla ROC, per la raccolta delle informazioni effettuata mediante trasmissione di documenti cartacei, sono tenuti ad adottare le seguenti misure di sicurezza:

a) i documenti cartacei devono essere inseriti in plico chiuso, inviati mediante corriere espresso, posta assicurata o recapito a mano, con garanzia di tracciabilità in fase di

trasporto e consegna del plico medesimo;

b) sul plico deve essere apposta la dicitura "Contiene dati personali. Riservato agli incaricati del trattamento dell' Ufficio "XXX"";
c) utilizzare plichi o "incarti" non trasparenti al fine di rendere inintelligibile il contenuto;
d) apporre una firma o sigla sui lembi di chiusura del plico.

E' in ogni caso vietato inviare via fax documenti contenenti dati oggetto del trattamento.

Con specifico riferimento alle operazioni di **registrazione** sulla Piattaforma sono adottate, dai Titolari e dai Centri partecipanti e Organizzazioni terze designate, misure di sicurezza, tecniche e organizzative, volte a garantire un livello di sicurezza adeguato al rischio e sono, inoltre, impiegati, dai soggetti coinvolti nelle attività di trattamento, ciascuno per la parte di propria competenza, in base al ruolo ricoperto e alle conseguenti responsabilità, specifiche misure volte ad elevare il livello di sicurezza dei dati trattati.

2.4.3 Fase di elaborazione dei dati

I dati raccolti nella Piattaforma sono trattati dagli autorizzati con le misure indicate e descritte attraverso adeguati sistemi di autenticazione e di autorizzazione in funzione del ruolo degli stessi autorizzati.

Con specifico riferimento alle operazioni di **elaborazione dei dati memorizzati** nella Piattaforma sono predisposte le seguenti misure:

- idonei sistemi di autenticazione e di autorizzazione per il personale preposto al trattamento in funzione dei ruoli ricoperti e delle esigenze di accesso e trattamento, utilizzando credenziali di validità limitata alla durata del trattamento in Piattaforma e disattivandole al termine della stessa;
- procedure per verificare periodicamente la qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati ai soggetti designati al trattamento;
- sistemi di *audit log* per il controllo degli accessi al *database* e per il rilevamento di eventuali anomalie.

In particolare, il trattamento dei dati personali degli Interessati registrati in Piattaforma verrà effettuato con i seguenti mezzi e modalità:

- i dati personali, compatibilmente a natura e finalità della ROC, saranno "pseudonimizzati" mediante l'utilizzo di un codice di identificazione pseudo-anonimo (progressivo univoco), in osservanza del principio di minimizzazione dei dati;
- il personale sanitario autorizzato non includerà informazioni personali eccedenti nella Piattaforma o in altre forme, file elettronici, pubblicazione o presentazione a un'autorità regolatoria;
- i titolari del trattamento potranno comunicare tra loro i dati personali registrati nella Piattaforma per le sole finalità relative alla ROC e alla relativa Piattaforma e se l'operazione di comunicazione sia indispensabile per la conduzione degli Studi;
- i dati relativi alla salute degli interessati non saranno diffusi né comunicati a soggetti esterni.

2.4.4 Fase di conservazione dei dati

I dati raccolti devono essere memorizzati e conservati in luoghi e con modalità prestabilite dai Titolari stesso, in modo tale da proteggere l'identità e tutelare la riservatezza degli Interessati.

I dati devono essere conservati con garanzie di riservatezza, integrità e disponibilità, con conseguente possibilità di ripristino dei dati stessi in caso di guasti e malfunzionamenti al fine di eventuali successive verifiche ed integrazione dei dati.

Il ripristino dei dati deve avvenire secondo una documentata procedura di restore, prestabilita dai Titolari del trattamento.

I supporti informatici e i documenti cartacei contenenti i dati della Piattaforma devono essere riposti dagli autorizzati in appositi archivi, organizzati secondo una documentata procedura relativa alla nomenclatura e alla classificazione dei supporti in modo che siano univocamente identificabili, soltanto attraverso apposito codice in caso di necessità e di verifica.

2.4.5 Fase di cancellazione dei dati e dismissione dei supporti

I dati presenti sul sistema informatico della Piattaforma devono essere cancellati o resi anonimi

in maniera irreversibile trascorso il periodo di trattamento e conservazione previsto dai Titolari

La procedura di anonimizzazione deve adottare tecniche adeguate alla protezione dell'identità dei pazienti da rischi legati all'identificabilità mediante individuazione, correlabilità e deduzione a partire dai dati sanitari.

Devono essere applicate tecniche di randomizzazione e generalizzazione dei dati, tenuto conto dell'evoluzione tecnologica.

I supporti informatici (es. memorie di massa dei server e delle postazioni di lavoro, supporti rimovibili etc..) devono essere dismessi secondo quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 sui "*Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali*" (G.U. n. 287 del 9 dicembre 2008) e s.m.i..

I supporti cartacei relativi alla ROC e alla Piattaforma, contenenti dati sanitari, devono essere distrutti secondo una documentata procedura, prestabilita dal Titolare del trattamento.

3. GESTIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI

3.1 La sicurezza dei dati trattati nella Piattaforma deve essere garantita in tutte le fasi del trattamento dei dati, mediante l'adozione degli opportuni accorgimenti volti a preservare i medesimi dati da rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Di seguito verranno indicate e descritte, in primo luogo, in modo sintetico, le misure tecniche funzionali alla protezione dei dati personali dei pazienti reclutati nella ROC e, in secondo luogo, in modo più analitico, le tecnologie e le procedure specificamente adottate per conseguire il medesimo fine.

3.1.1 MISURE DI SICUREZZA ESISTENTI E PIANIFICATE

- La Piattaforma è sviluppata e configurata appositamente per ridurre al minimo l'utilizzazione dei dati personali al di fuori delle finalità della ROC.

- Attraverso i protocolli http e SSL con accesso tramite username e password sono garantiti elevati livelli di sicurezza e riservatezza delle informazioni, assicurando la trasmissione dei dati tramite un canale di connessione sicuro e cifrato.

- I dati caricati in Piattaforma sono pseudonimizzati e, in ogni caso, la riservatezza ed integrità degli stessi è garantita da un robusto sistema di log degli accessi e delle operazioni svolte dalle persone dotate dei privilegi di AdS (di amministratore della Piattaforma) che consente di svolgere a posteriori azioni di auditing sulla liceità dei trattamenti attuati dalla FONDAZIONE PASCALE quale gestore/detentore della Piattaforma elettronica.

- I futuri sviluppi della Piattaforma dovranno essere validati sotto il profilo della sicurezza informatica da adeguate azioni di vulnerability assessment attuate prima della messa in esercizio, per individuare e correggere eventuali vulnerabilità nell'utilizzo della stessa prima di renderla fruibile ai Centri partecipanti e agli altri utenti e le verifiche sulla tenuta ed efficacia delle misure di sicurezza saranno periodicamente rinnovate, per garantire, nel tempo, un livello costante di protezione dei dati personali.

- Le credenziali di autenticazione sono assegnate ad uso esclusivo di ciascun utente definendo per ciascuno i differenti profili di autorizzazione

- L' autenticazione informatica degli utenti viene effettuata mediante un sistema multifattori e, in ogni caso, le password relative agli utenti saranno di lunghezza non inferiore a 12 caratteri e sottoposte a un controllo automatico di qualità che impedisce l'uso di password deboli costituite, ad esempio, da parole reperibili in dizionari o comunque facilmente individuabili; sono previste, inoltre, strette limitazioni al numero di tentativi di accesso alla Piattaforma con password erronea, per impedire attacchi brute forze interattivi.

- Le misure di auditing per la verifica della liceità dei trattamenti compiuti dagli incaricati dotati di profili di autorizzazione ampi e speciali consentono nella tenuta delle registrazioni degli accessi e delle operazioni compiute (log) sil database, attuando gli accorgimenti di cui al Provvedimento generale del Garante del 27/11/2008 in tema di amministratori di sistema (adS).

- Terminato il periodo di conservazione, sarà attivato un meccanismo di anonimizzazione previsto per rimuovere le informazioni riferibili agli Interessati o trasformarle in forma anonima.

3.1.2 TECNOLOGIE E PROCEDURE ESISTENTI E PIANIFICATE

La FONDAZIONE PASCALE, al fine di garantire il rispetto dei principi di riservatezza, integrità e disponibilità dei dati personali inerenti alla ROC, adotta tecnologie e procedure per:

3.1.2.1 il controllo degli accessi;

3.1.2.2 l'autenticazione sicura;

3.1.2.3 la raccolta e gestione dei log;

3.1.2.4 la classificazione delle informazioni;

3.1.2.5 il mascheramento dei dati, la pseudonimizzazione e l'anonimizzazione;

3.1.2.6 la gestione, la valutazione e la risposta in ordine alle vulnerabilità tecniche;

3.1.2.7 il backup delle informazioni

3.1.2.1 Controllo degli accessi

Conformemente alla politica da applicarsi a tutti i sistemi IT della Fondazione Pascale il **controllo degli accessi logici** alla Piattaforma ROC e ai correlati sistemi informatici definisce gli aspetti relativi a: autenticazione informatica (il processo tramite cui un sistema informatico verifica la corretta identità di un altro computer, software o utente); attribuzione di ruoli e responsabilità che attengono al sistema di controllo degli accessi; adozione di processi di autorizzazione e di aggiornamento periodico delle autorizzazioni; controllo degli accessi ai sistemi informatici e ai dati, rilevazione di eventuali azioni non consentite

La **politica sul controllo per gli accessi** si applica, per quanto possibile, alla Fondazione Pascale, a tutto il personale interno, ai Titolari del trattamento e alle terze parti che utilizzano la Piattaforma nonché a tutti i processi e risorse coinvolte nella progettazione, realizzazione ed erogazione dei servizi clinico - scientifici inerenti alla ROC.

Lo scopo è garantire la protezione del patrimonio informativo della ROC da minacce e rischi garantendo la continuità dei servizi clinici e sanitari e la realizzazione di progetti di ricerca scientifica.

I principi generali per l'accesso alla Piattaforma ROC sono i seguenti:

- l'accesso ai dati è vietato, fatte salve espresse autorizzazioni per utenti determinati e formale registrazione; le credenziali di autenticazione consistono in un codice per l'identificazione dell'autorizzato (username) associato a una parola chiave riservata conosciuta soltanto dal medesimo (password); ad ogni autorizzato è assegnata una credenziale per l'autenticazione; il codice per l'identificazione non può essere assegnato ad altra persona fisica, neppure in tempi diversi; le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle relative alla sola gestione tecnica; le credenziali sono disattivate anche in caso di perdita della qualità che legittimava la persona all'accesso ai dati (cambiamento mansioni, cessazione del rapporto di lavoro); gli assegnatari delle password devono conservarle diligentemente, escludendo che possano essere lette, volontariamente o involontariamente, da altre persone; il personale deve utilizzare esclusivamente le proprie utenze e non cedere mai i propri codici

identificativi e password ad altri soggetti.

L'accesso alla Piattaforma e ai sistemi informatici è controllato da **procedure di monitoraggio** conformi alla Politica sui log relativi alla Piattaforma per assicurare che l'accesso alle informazioni sia effettuato esclusivamente dai soggetti autorizzati, rilevando eventuali tentativi di accesso non consentiti attraverso:

- l'adozione di sistemi idonei alla registrazione degli accessi logici (access log) alla Piattaforma e agli archivi elettronici da parte degli amministratori di sistema e, ove possibile, degli autorizzati;
- le registrazioni degli accessi devono presentare caratteristiche di completezza (riferimenti temporali, descrizione dell'evento, utenza associata), inalterabilità, verificabilità;
- le registrazioni devono essere conservate per un congruo periodo, quantomeno un anno per gli Amministratori di Sistema.

Le seguenti **attività di accesso alla Piattaforma ROC** e ai correlati sistemi informatici devono essere **registrate:** tentativi di accesso andati a buon fine (log on); tentativi di accesso falliti; durata dell'accesso (log off).

L'assegnazione, l'uso e la revoca di diritti di accesso degli utenti alla Piattaforma vengono attuati e gestiti tramite un **processo formale** di richiesta, autorizzazione e assegnazione degli account; i diritti di accesso devono essere individuati e configurati anteriormente all'abilitazione dell'accesso per gli utenti, limitandone l'accesso alle sole funzionalità/dati necessari per effettuare le operazioni previste evitando che a un medesimo utente siano stati abilitati account con ruoli che presentino e/o siano suscettibili di presentare conflitto di interesse (controllato/controllore)

L'assegnazione, l'uso e la revoca di **diritti di accesso privilegiato** (amministratore di sistema) sono limitati e controllati tramite un processo formale di richiesta, autorizzazione e assegnazione degli account

Le utenze di amministrazione dei sistemi devono essere attribuite solo a personale che sia stato formalmente designato del ruolo di "Amministratore di Sistema" ai sensi dei pertinenti Provvedimenti del Garante privacy e non sono utilizzate per lo svolgimento di mansioni personali che esulano dall'amministrazione dei sistemi.

I **diritti di accesso** degli utenti della Piattaforma sono regolarmente **riesaminati**, ad intervalli regolari, per verificare la persistenza delle condizioni per conservare i profili di autorizzazione.
I **diritti di accesso** alla Piattaforma devono essere **rimossi** al momento della cessazione del rapporto di lavoro o di collaborazione e tali diritti devono essere adattati ad ogni variazione di tipo organizzativo o contrattuale.
Tutti gli utenti della Piattaforma devono: mantenere riservate le informazioni di autenticazione per l'accesso alla Piattaforma; evitare di salvare le informazioni di autenticazione su carta, su documenti software o dispositivi portatili; modificare la password di autenticazione ogni qualvolta vi sia un sospetto della sua possibile compromissione; segnalare eventuali rischi o incidenti di sicurezza relativi agli account.
Sono **documentati e registrati** gli accessi e tutti gli eventi inerenti al ciclo di vita delle utenze per l'accesso alla Piattaforma (Registrazione della richiesta e assegnazione dei privilegi).
Le registrazioni non possono essere modificate e sono conservate per un periodo di 3 anni.

3.1.2.2 Autenticazione sicura

Le tecnologie e le procedure di autenticazione sicura sono attuate in base alle limitazioni degli accessi alle informazioni e alla politica specifica per il controllo degli accessi al fine di assicurare che gli utenti della Piattaforma ROC siano autenticati in modo sicuro quando viene loro concesso l'accesso.
Sono scelte tecniche di autenticazione adeguate per comprovare l'identità dichiarata dagli utenti e la robustezza dell'autenticazione è adeguata al carattere sensibile delle informazioni a cui accedere.
E’ preferibilmente implementata l'autenticazione forte verificando l'identità mediante metodi di autenticazione alternativi alle password (certificati digitali, smart card, token).
La FONDAZIONE PASCALE considera, infatti, che l'utilizzo di una combinazione di più fattori di autenticazione (ciò che si sa, ciò che si ha) riduce le possibilità di accessi non autorizzati.
Le procedure e le tecnologie di accesso sono attuate tenendo conto di quanto segue:
non visualizzare informazioni sensibili di sistema o dell’applicazione fino a quando il processo di accesso non è stato completato con successo al fine di evitare di fornire assistenza non

necessaria a un utente non autorizzato; visualizzare un avviso generale con l'avvertenza che l'accesso al sistema o all'applicazione o al servizio è riservato agli utenti autorizzati; non fornire messaggi di aiuto durante la procedura di accesso che possano aiutare un utente non autorizzato (se si verifica una condizione di errore, il sistema non indica quale parte dei dati è corretta o non corretta); convalidare le informazioni di accesso solo al completamento di tutti i dati inseriti; proteggere contro i tentativi di accesso a forza bruta su username e password (richiedendo il ripristino della password dopo un numero predefinito di tentativi falliti o bloccando l'utente dopo un numero massimo di errori); registrare i tentativi falliti e riusciti; segnalare un evento relativo alla sicurezza se viene rilevata una possibile violazione tentata o riuscita dei controlli di accesso (invio di un avviso all'utente e agli amministratori di sistema dell'organizzazione quando è stato raggiunto un certo numero di tentativi di password errati); non visualizzare la password in chiaro al momento dell'inserimento; non trasmettere le password in chiaro su una rete per evitare che siano catturate da un programma "sniffer" di rete; terminare le sessioni inattive dopo un periodo di inattività definito.

3.1.2.3 Raccolta e gestione dei log

Conformemente alla politica da applicarsi a tutti i sistemi IT della Fondazione Pascale, i log di sicurezza, nell'ambito del trattamento dei dati personali relativo alla ROC e alla sua Piattaforma, sono generati, gestiti e conservati in modo da supportare il monitoraggio continuo e la risposta agli incidenti di sicurezza e a eventuali data breach.

I log di sicurezza generati e raccolti devono: **registrare eventi significativi (**tentativi di accesso riusciti e falliti; accessi privilegiati ai sistemi; modifiche a file di configurazione, applicazioni o database; tentativi di modifica o eliminazione dei log stessi; anomalie che possono indicare tentativi di intrusione o compromissione); essere **protetti** da accessi non autorizzati, alterazioni o distruzioni accidentali o dolose (mediante misure idonee a garantire (firma digitale, hashing) l'integrità dei dati; essere **cifrati** sia durante la trasmissione che durante la conservazione; sottoposti a **backup regolari e conservati** in un ambiente sicuro per un periodo minimo di 12 mesi; essere **monitorati** attivamente e in tempo reale con strumenti di monitoraggio automatico in grado di: identificare schemi di comportamento anomali (accesso

simultaneo a più sistemi da luoghi geograficamente distanti); correlare eventi attraverso diversi sistemi per rilevare attacchi avanzati o persistenti; inviare notifiche automatiche al team di sicurezza IT in caso di eventi critici.

Per garantirne l'integrità e prevenire accessi non autorizzati, **l'accesso ai log** deve essere **limitato** al personale autorizzato e ogni accesso ai log deve essere registrato e monitorato.

Le **revisioni periodiche dei log** garantiscono che le anomalie rilevate siano adeguatamente analizzate e documentate e che le misure correttive siano state adottate

In caso di violazioni dei dati personali e, in generale, incidenti di sicurezza i log devono essere utilizzati per l'indagine e conservati integri per tutta la durata della stessa e, ove occorra, per un periodo prolungato.

Tutti gli incidenti che comportano una compromissione dei log stessi devono essere segnalati

Gli **audit relativi ai log** devono: valutare se i log vengono raccolti, protetti e conservati correttamente; verificare l'integrità dei log; controllare che le misure di protezione e monitoraggio siano correttamente implementate.

3.1.2.4 Classificazione delle informazioni

I dati relativi alla ROC e alla sua Piattaforma sono **classificati e protetti** coerentemente alla loro natura (dati particolari "sensibili", relativi alla salute) e al loro livello di criticità (dati relativi a soggetti vulnerabili) individuando e limitando il numero di persone che possono accedere alle singole informazioni e le attività che possono compiere sulle informazioni stesse secondo le regole del "minimo privilegio" e del "need to know".

Il livello di classificazione attribuito a tali dati tiene conto del danno potenziale derivante da una divulgazione non autorizzata delle informazioni, innalzando, dunque, il livello di classificazione attribuito.

Il livello di classificazione individuato viene indicato ed evidenziato tramite procedura di etichettatura.

3.1.2.5 Mascheramento, pseudonimizzazione e anonimizzazione dei dati

Al fine di limitare l'esposizione dei dati sensibili relativi ai pazienti registrati nella Piattaforma, e in ragione delle criticità del trattamento in esame, la FONDAZIONE

PASCALE utilizza tecniche come il **mascheramento dei dati, la pseudonimizzazione o l'anonimizzazione** le quali implicano, peraltro, la verifica che i dati siano stati adeguatamente mascherati, pseudonimizzati o resi anonimi.

La FONDAZIONE PASCALE utilizza, inoltre, le seguenti tecniche aggiuntive per il mascheramento dei dati: occultamento o eliminazione di caratteri (impedendo agli utenti non autorizzati di vedere i messaggi completi); numeri e date variabili; sostituzione (cambiamento di un valore con un altro per nascondere dati sensibili).

L'IRCCS PASCALE, infine, non concede a tutti gli utenti l'accesso a tutti i dati (query e maschere mostrare all'utente solo i dati minimi richiesti); in alcuni casi, al personale ospedaliero vengono presentati dati parzialmente offuscati e i dati sono accessibili al personale con ruoli specifici solo se contengono informazioni utili per un trattamento appropriato.

Quando si utilizza il mascheramento dei dati, la pseudonimizzazione o l'anonimizzazione, la FONDAZIONE PASCALE considera quanto segue: livello di efficacia del mascheramento, pseudonimizzazione o anonimizzazione dei dati in base all'utilizzo dei dati trattati; controlli di accesso ai dati trattati; limitazioni all'utilizzo dei dati trattati; vietare di confrontare i dati trattati con altre informazioni al fine di identificare l'interessato dei dati personali.

La pseudonimizzazione, ove applicabile, verrà eseguita nel seguente modo:

- i dati raccolti saranno trattati con la massima riservatezza e saranno pseudonimizzati con un codice univoco attribuito ai singoli Interessati;
- il codice univoco non includerà nessun dato personale direttamente riconducibile ai pazienti (nome, cognome o numero di cartella clinica o numero di telefono) e sarà utilizzato al posto del nome dei pazienti e di altre informazioni che direttamente e facilmente li identifichino;
- il documento contenente le informazioni che permettono di decifrare i codici e risalire all'identità dei pazienti (mediante il collegamento tra i dati personali dei pazienti ed i dati pseudonimizzati) sarà detenuto esclusivamente da ciascun Centro partecipante che dovrà

custodirlo come documento riservato essenziale tenuto conto degli artt. 4, par. 1, n. 5 e 32 Reg. UE 2016/679.

L'anonimizzazione verrà effettuata al termine del periodo di conservazione attraverso un processo mediante il quale i dati personali verranno modificati in modo irreversibile (al fine di ridurre sensibilmente il rischio di re-identificazione dei pazienti), tenendo conto di quanto previsto nel *Parere 5/2014* del Gruppo di lavoro art. 29, nelle tecniche di pseudonimizzazione Enisa, nel Codice di Condotta approvato il 14 gennaio 2021

L'anonimizzazione dei dati sarà ottenuta attraverso plurime metodologie finalizzate a minimizzare il rischio di re-identificazione dei soggetti coinvolti nella Piattaforma.

3.1.2.6 Gestione, valutazione e risposta alle vulnerabilità tecniche.

Al fine di prevenire lo sfruttamento delle vulnerabilità tecniche, la FONDAZIONE PASCALE ricerca, monitora e verifica le vulnerabilità tecniche della Piattaforma ROC, valutando l'esposizione dell'Organizzazione a tali vulnerabilità e adottando misure appropriate.

Per raggiungere tale obiettivo e identificare le vulnerabilità tecniche, l'IRCCS PASCALE dispone di un accurato inventario degli asset come prerequisito per un'efficace gestione tecnica delle vulnerabilità e inoltre deve:

- definire e stabilire i ruoli e le responsabilità associati alla gestione delle vulnerabilità tecniche, compreso il monitoraggio delle vulnerabilità, la valutazione del rischio di vulnerabilità, l'aggiornamento, il tracciamento degli asset e le eventuali responsabilità di coordinamento richieste; sulla base dell'inventario degli asset, identificare le risorse informative che vengono utilizzate per identificare le vulnerabilità tecniche pertinenti e mantenere la consapevolezza su di esse; aggiornare l'elenco delle risorse informative in base ai cambiamenti nell'inventario o quando vengono trovate altre risorse nuove o utili; utilizzare strumenti di scansione delle vulnerabilità adeguati alle tecnologie in uso per identificare le vulnerabilità e verificare se l'installazione delle patch delle vulnerabilità ha avuto successo; condurre penetration test o vulnerability assessment pianificati, documentati e ripetibili da parte di soggetti competenti e autorizzati a supporto dell'identificazione delle vulnerabilità.

Per **valutare** le vulnerabilità tecniche identificate, la FONDAZIONE PASCALE adotta le seguenti misure: a) analizza e verifica i rapporti di segnalazione per determinare quale attività di risposta e di remediation è necessaria; b) una volta individuata una potenziale vulnerabilità tecnica, individua i rischi connessi e le azioni da intraprendere (che possono comportare l'aggiornamento di sistemi vulnerabili o l'applicazione di altri controlli); adotta misure adeguate per fronteggiare le vulnerabilità tecniche.

Per **fronteggiare** le vulnerabilità tecniche l'IRCCS PASCALE: intraprende azioni adeguate e tempestive in risposta all'identificazione di potenziali vulnerabilità tecniche; definisce una sequenza temporale per reagire alle notifiche di vulnerabilità tecniche potenzialmente pertinenti; utilizza solo aggiornamenti da fonti legittime (che possono essere interne o esterne all'organizzazione); testa e valuta gli aggiornamenti prima della loro installazione per assicurare che siano efficaci e non determinino effetti collaterali non tollerabili; individua remediation (sotto forma di aggiornamenti software o di patch) e conduce test per confermare se la remediation o la mitigazione sono efficaci; fornisce meccanismi per verificare l'autenticità della remediation.

Ove l'aggiornamento non sia disponibile o non possa essere installato, la FONDAZIONE PASCALE: applica qualsiasi soluzione alternativa suggerita dal fornitore del software o da altre fonti pertinenti; disattiva servizi o funzionalità legate alla vulnerabilità; adatta o aggiunge controlli di accesso (per esempio firewall) ai confini della rete; protegge la Piattaforma dalla vulnerabilità degli attacchi tramite la configurazione di filtri di traffico adeguati; aumenta il monitoraggio per rilevare gli attacchi effettivi; aumenta la consapevolezza della vulnerabilità.

Infine, la FONDAZIONE PASCALE: conserva un log per tutte le fasi intraprese nella gestione delle vulnerabilità tecniche; monitora il processo di gestione delle vulnerabilità tecniche al fine di assicurarne l'efficacia e l'efficienza; allinea, per quanto possibile, il processo di gestione delle vulnerabilità tecniche con le attività di gestione degli incidenti, per comunicare i dati sulle vulnerabilità alla funzione di risposta agli incidenti e fornire procedure tecniche da seguire in caso di incidente.

3.1.2.7 Backup delle informazioni

Conformemente alla politica da applicarsi a tutti i sistemi IT della Fondazione Pascale, il processo di salvataggio e ripristino dei dati inerenti alla Piattaforma ROC assicura la loro disponibilità in caso di necessità e, a tal fine, la FONDAZIONE PASCALE: definisce regole per la gestione strutturata dei processi di backup (procedura di sicurezza delle informazioni volta a garantirne la disponibilità) e restore (operazione di ripristino dello stato originario dei sistemi) delle informazioni, per prevenire la perdita di dati in caso di cancellazione o corruzione dei file; definisce regole, ruoli e responsabilità che attengono alla gestione di backup e restore.

La politica di **backup** si applica alla Piattaforma ROC utilizzata dal personale autorizzato, esterno o interno alla Fondazione Pascale.

Per assicurarne **l'integrità e la disponibilità**, i dati registrati nella Piattaforma ROC sono oggetto di salvataggio e ripristino intesi (sotto il profilo della data protection) come ulteriori trattamenti da gestire in conformità alla normativa vigente, evitando accessi non legittimati dalle operazioni di backup e restore.

Nell'ambito del **piano di backup predisposto per la ROC,** gli obiettivi del backup sono individuati in termini di: Recovery Point Objective (**RPO**): determinato dal momento in cui si effettua l'ultimo backup prima di un disastro; Recovery Time Objective (**RTO**): determinato dalla quantità di tempo trascorso tra il disastro e il ripristino delle funzioni aziendali.

La FONDAZIONE PASCALE, esegue le seguenti fasi: definizione dei cicli di backup; definizione del numero di copie; definizione della durata della conservazione delle varie copie (retention); redazione del piano di backup mensile

Le **modalità di realizzazione del backup**, con riferimento alla Piattaforma ROC, sono le seguenti:

Backup di primo livello (completo): vengono salvati su altro supporto i dati nella loro totalità, con la cadenza ritenuta opportuna (si conservano almeno tre copie); le operazioni di backup di primo livello vanno effettuate a sistema chiuso per gli utenti e

preferibilmente alla fine della giornata lavorativa.

Backup di secondo livello (incrementale): vengono salvati solo gli aggiornamenti e/o le variazioni ai dati di partenza (gli aggiornamenti vengono accumulati per tutto il periodo prescelto rispetto ai backup di secondo livello e possono essere effettuati durante l'intera giornata lavorativa, in contemporanea con l'attività dell'utente).

Il **restore**, quale operazione di ripristino dello stato originario dei sistemi, viene effettuato, utilizzando le copie di backup nel seguente modo:

Richiesta di ripristino ordinaria: per richiedere il restore occorre fornire le seguenti informazioni: motivo del restore; nome del file o della cartella (directory) da ripristinare; locazione originaria della cartella o del file; data e orario presunto della cancellazione/corruzione dei file/cartelle da ripristinare; ultima data e ora in cui l'utente ricorda di aver avuto accesso al file/cartella integri.

Ripristino di emergenza: in caso di disastro verrà avviata una richiesta di ripristino di emergenza

I test di ripristino **del backup** devono essere avviati su base periodica (almeno mensile) per garantire che lo schema di backup funzioni come previsto.

3.2 ACCESSO ILLEGITTIMO AI DATI

Se il rischio di accesso illegittimo ai dati personali dovesse concretizzarsi, ci potrebbero essere impatti significativi sugli Interessati.

L'accesso illegittimo potrebbe compromettere la privacy dei pazienti interessati, esponendo informazioni personali sensibili a terze parti non autorizzate.

Ciò potrebbe comportare una violazione della riservatezza e dell'autonomia degli Interessati.

I dati personali potrebbero essere utilizzati in modo improprio (ad esempio, per attività di frode o di furto di identità) mettendo gli Interessati a rischio di danni reputazionali; l'utilizzo improprio dei dati potrebbe anche portare a discriminazioni o pregiudizi nei confronti dei pazienti interessati.

L'accesso illegittimo ai dati personali potrebbe compromettere la sicurezza delle informazioni e rendere gli Interessati vulnerabili sotto diversi aspetti.

Gli Interessati potrebbero perdere il controllo sui propri dati personali e sulla loro diffusione; ciò potrebbe minare la fiducia dei pazienti interessati nel trattamento dei loro dati, compromettendo l'efficacia e l'attendibilità della ROC e della Piattaforma con conseguente perdita di chance per i malati.

Potrebbe, inoltre, determinarsi una violazione dell'autodeterminazione informativa degli interessati cui verrebbe precluso l'esercizio del diritto a decidere liberamente e consapevolmente se e come partecipare alla ROC e se autorizzare alla registrazione in Piattaforma

3.2.1 Le principali minacce che potrebbero concretizzare il rischio.

Le principali minacce che potrebbero concretizzare il rischio di accesso illegittimo ai dati includono:

a) i criminali informatici possono tentare di penetrare nei sistemi informatici al fine di accedere ai dati personali;
b) gli attacchi informatici (phishing, malware, ransomware, attacchi DDoS) possono essere attuati dagli aggressori sfruttando le vulnerabilità della Piattaforma e/o dei sistemi
c) i malintenzionati potrebbero cercare di ottenere informazioni sensibili come password o dati personali, inviando comunicazioni fraudolente che sembrano provenire da fonti affidabili;
d) persone interne alle organizzazione coinvolte nel trattamento dei dati come dipendenti disonesti o negligenti, potrebbero abusare o divulgare dati sensibili;
e) persone interne all'organizzazione coinvolte nel trattamento dei dati ma non autorizzate ad accedere a specifici locali e/o reparti potrebbero abusare o divulgare dati sensibili;

f) l’assenza di sorveglianza degli accessi alla Piattaforma e/o l’accesso di terzi alla Piattaforma e ad aree e/o reparti nei quali viene iniziato e/o gestito il trattamento potrebbe determinare l’illecito utilizzo di dati sensibili;
g) l’assenza di informazioni specifica per gli incaricati potrebbero causare l’illecito trattamento dei dati;
h) la mancanza di adeguate procedure e misure di sicurezza, l’omesso aggiornamento o l’obsolescenza delle stesse potrebbero facilitare l'accesso illegittimo ai dati;
i) la mancanza di misure di sicurezza fisica potrebbe consentire l'accesso illegittimo ai dati;
j) l'accesso non autorizzato o l’abuso dei privilegi amministrativi o di altro personale autorizzato può compromettere la sicurezza dei dati;
k) la mancanza di adeguati controlli di accesso e di autenticazione può facilitare l'accesso illegittimo ai dati;
l) l’inconsapevolezza degli utenti della Piattaforma sulle pratiche di sicurezza e il conseguente rischio di inganno degli utenti coinvolti nella ROC può causare l’illegittimo trattamento dei dati
m) il furto o la perdita di dispositivi contenenti dati sensibili possono favorire l’accesso illegittimo ai dati personali;

3.2.2 Le fonti di rischio.

Le fonti di rischio per l'accesso illegittimo ai dati possono derivare da diverse situazioni o fattori.

Alcune delle principali fonti di rischio includono:

a) le vulnerabilità tecniche o di sicurezza presenti nella Piattaforma e nei sistemi informatici coinvolti nelle attività relative alla ROC;
b) la mancanza di adeguate misure di protezione dei dati;
c) errori commessi da personale interno possono rappresentare una fonte di rischio per l'accesso non autorizzato;

d) la negligenza, omissioni e/o intenti fraudolenti degli incaricati e l'omessa o negligente gestione e manutenzione della Piattaforma e dei relativi asset.

3.2.3 Le misure che contribuiscono a mitigare il rischio.

Per mitigare il rischio di accesso illegittimo ai dati personali, all'interno della Piattaforma sono state adottate una serie di misure di sicurezza, descritte nei precedenti paragrafi di questo documento:

a) accesso limitato e controllato ai dati personali del solo personale autorizzato sia a livello fisico che informatico;
b) pseudonimizzazione dei dati e comunicazione degli stessi tramite chiave crittografica;
c) protezione fisica dell'infrastruttura informatica utilizzata;
d) monitoraggio e rilevamento delle intrusioni nella Piattaforma e nei sistemi informativi;
e) definizione di politiche e procedure di sicurezza relative a tutti i soggetti coinvolti nella Piattaforma: titolari, responsabili, designati e autorizzati;
f) formazione del personale coinvolto sui rischi associati all'accesso illegittimo ai dati personali;
g) audit e controllo delle attività svolte da responsabili e referenti.

3.2.4 Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate.

Le minacce individuate nei punti precedenti sonostate valutate in base alla loro frequenza, alla loro complessità e alla loro capacità di superare le misure di sicurezza adottate. Considerando l'elevata frequenza di eventi di data breach nel settore dei dati sanitari, la probabilità del rischio è da considerarsi importante. Tuttavia, le misure pianificate, come sopra descritte, contribuiscono a mitigare il rischio di accesso illegittimo.

3.2.5 Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate.

In ragione della sensibilità dei dati trattati e degli impatti potenziali, l'accesso illegittimo ai dati personali potrebbe causare importanti violazioni dei diritti fondamentali degli Interessati.

Tuttavia, le misure pianificate per mitigare il rischio di accesso illegittimo ai dati, indicate e descritte nel precedente punto 3.2.3 e nei paragrafi precedenti e l'adozione di politiche e procedure di sicurezza contribuiscono a ridurre significativamente la gravità del rischio.

3.3 MODIFICHE INDESIDERATE DEI DATI

Se il rischio di modifiche indesiderate dei dati personali dovesse concretizzarsi, ci potrebbero essere impatti significativi sugli Interessati come di seguito riportati.

Le modifiche indesiderate potrebbero alterare in modo errato o distorto i dati personali, compromettendo la loro accuratezza e affidabilità; ciò potrebbe influire sulla qualità e sull'affidabilità delle informazioni utilizzate nella ROC e nella relativa Piattaforma, portando a conclusioni errate o inesatte.

I Centri partecipanti, la Fondazione Pascale e soprattutto i pazienti interessati potrebbero perdere fiducia nella correttezza e nell'integrità dei dati personali raccolti e trattati nella Piattaforma e ciò potrebbe influenzare la loro partecipazione alla ROC la volontà di condividere informazioni sensibili.

Le modifiche indesiderate ai dati personali potrebbero influenzare negativamente le decisioni cliniche prese nell'ambito della Piattaforma; se le informazioni modificate venissero utilizzate per formulare diagnosi o piani di trattamento, potrebbe esserci un impatto sulla salute e sulla sicurezza degli Interessati.

Le modifiche indesiderate dei dati potrebbero portare a discriminazioni o pregiudizi nei confronti degli Interessati; ad esempio, se le informazioni fossero alterate in modo da creare false rappresentazioni di una condizione medica o di un rischio associato, gli Interessati potrebbero subire conseguenze negative.

Le modifiche indesiderate dei dati potrebbero avere conseguenze legali per i Centri partecipanti e per la Fondazione che gestisce la Piattaforma con conseguenti perdite di

servizi e chance per i pazienti.

Potrebbero essere necessarie azioni legali per correggere gli errori o le distorsioni dei dati, oltre a possibili richieste di risarcimento danni o azioni legali avanzate da parte degli Interessati a seguito di tali modifiche indesiderate.

3.3.1 Le principali minacce che potrebbero concretizzare il rischio.

Le principali minacce che potrebbero concretizzare il rischio di modifiche indesiderate dei dati includono:

a) criminali informatici possono tentare di penetrare nei sistemi informatici al fine di modificare i dati personali;
b) persone interne all'organizzazione coinvolta nel trattamento dei dati, come dipendenti o amministratori di sistema, potrebbero abusare dei propri privilegi di accesso per apportare volontariamente modifiche non autorizzate ai dati personali ovvero apportare accidentalmente modifiche non autorizzate;
c) gli incaricati coinvolti nel trattamento potrebbero inserire o modificare i dati personali in modo non accurato o non completo;
d) in generale, errori umani, come la manipolazione erronea dei dati o l'inserimento di informazioni errate, potrebbero portare a modifiche indesiderate dei dati;
e) l'infezione da malware, come virus, worm o ransomware, potrebbe compromettere la sicurezza dei sistemi informatici e consentire agli aggressori di apportare modifiche indesiderate ai dati personali;
f) durante il trasferimento dei dati da un sistema all'altro, potrebbero verificarsi vulnerabilità che consentono la manipolazione non autorizzata dei dati;
g) l'omessa custodia del pc e/o dei supporti di memorizzazione e l'omessa attribuzione agli incaricati di pc aziendali strutturati con specifiche misure di sicurezza potrebbero determinare modifiche indesiderate dei dati;
h) la negligenza dei soggetti autorizzati al trattamento dei dati sulla Piattaforma potrebbe causare alterazioni dei dati;

i) l’omesso aggiornamento e l’obsolescenza dei dati personali e dei moduli di informativa/consenso potrebbero concretizzare il rischio in esame;
j) errori, modifiche e/o omissioni nelle operazioni di gestione e archiviazione dei consensi sono possibili cause di illecito trattamento dei dati personali;
k) gli attacchi informatici, come malware, virus o ransomware, potrebbero compromettere la sicurezza dei sistemi informatici e consentire a terze parti di apportare modifiche indesiderate ai dati;
l) durante l’accesso in Piattaforma da parte dei professionisti sanitari dei Centri partecipanti e durante il trasferimento dei dati da un sistema all'altro su reti non sicure o durante l'elaborazione dei dati da parte di terze parti coinvolte nel trasferimento, potrebbero verificarsi vulnerabilità;

3.3.2 Le fonti di rischio.

Le fonti di rischio per le modifiche indesiderate dei dati possono derivare da diverse situazioni o fattori.

Alcune delle principali fonti di rischio includono:

a) gli errori commessi dagli operatori durante l'inserimento, la manipolazione o la gestione dei dati;
b) l'accesso non autorizzato da parte di individui o entità esterne;
c) l’abuso dei propri privilegi di accesso da parte delle persone interne alle organizzazioni coinvolte nel trattamento dei dati;
d) le persone interne alle organizzazioni potrebbero impropriamente accedere alla Piattaforma o commettere errori per sovraccarico di lavoro;
e) la negligente esecuzione delle operazioni di data entry nella Piattaforma;
f) la mancanza di adeguate misure di sicurezza contro le vulnerabilità dei dati personali;
g) l’assenza di una policy condivisa di utilizzo dei dispositivi elettronici;
h) l’assenza della cifratura sui dati dei pc personali eventualmente utilizzati;

i) l’assenza di procedure di ripristino dei dati e/o errori nell'attuazione delle procedure
j) l’utilizzo (non autorizzato dai titolari) di supporti esterni recanti i dati dei soggetti arruolati o l’utilizzo di credenziali d’accesso non segrete;
k) utilizzo, da parte degli operatori coinvolti dei propri pc personali (non autorizzati dai titolari) per le attività funzionali ai servizi della ROC;
l) la mancata conoscenza, da parte degli incaricati delle modalità di raccolta e conservazione di informative e consensi;
m) l’assenza di una policy specifica di gestione dei data breach e delle violazioni dei dati personali;
n) la mancata conoscenza da parte degli incaricati delle modalità per segnalare casi di violazione dei dati;
o) l’omessa o tardiva adozione di contromisure tempestive per evitare l’aggravio di conseguenze dannose per i diritti e le libertà degli interessati.

3.3.3 Le misure che contribuiscono a mitigare il rischio.

Per mitigare il rischio di modifiche indesiderate dei dati, all’interno della Piattaforma sono adottate una serie di misure di sicurezza descritte anche nei punti precedenti della presente VIP:

a) implementare un sistema di gestione degli accessi che permetta solo alle persone autorizzate di accedere ai dati e limitare i privilegi di accesso in base al ruolo e alle responsabilità dell'utente;
b) utilizzare strumenti di monitoraggio e rilevamento delle attività anomale sulla Piattaforma per identificare potenziali tentativi di modifiche indesiderate o accessi non autorizzati;
c) implementare procedure per la gestione delle modifiche ai dati, compresa l'autorizzazione delle modifiche e la verifica dell'integrità dei dati;
d) effettuare regolari backup dei dati che consentano il ripristino in caso di manomissione;

e) implementare sistemi di autenticazione per garantire che solo le persone autorizzate possano accedere ai dati;
f) utilizzare la pseudonimizzazione e la criptazione delle comunicazioni in modo che anche se i dati vengono compromessi, non possono essere letti o utilizzati da persone non autorizzate;
g) fornire formazione sulla sicurezza dei dati a tutti i dipendenti coinvolti nel trattamento dei dati;
h) implementare politiche e procedure di sicurezza che stabiliscano le responsabilità, i ruoli e le azioni da intraprendere per garantire la protezione dei dati;
i) effettuare regolare monitoraggio delle attività dei soggetti coinvolti come responsabili, designati e autorizzati.;
j) adottare procedure specifiche su data breach e violazioni dei dati personali

3.3.4 Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate.

Le minacce individuate nei punti precedenti devono essere valutate in base alla loro frequenza, alla loro complessità e alla loro capacità di superare le misure di sicurezza adottate. Considerando l'elevata probabilità di errori umani, di negligenza del personale o di attacchi informatici nel settore dei dati sanitari, la probabilità del rischio è da considerarsi importante. Tuttavia, le misure pianificate, come sopra descritte, contribuiscono a mitigare il rischio di modifiche indesiderate dei dati.

3.3.5 Stime della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate.

La sensibilità dei dati trattati e il potenziale impatto sulle persone interessate rendono la gravità del rischio di modifiche indesiderate e non autorizzate dei dati personali considerabile come importante in quanto potrebbe compromettere l'integrità delle informazioni degli interessati con gravi conseguenze come evidenziato nei paragrafi precedenti di questo documento.

L'impatto negativo sulla salute dei soggetti arruolati nella Piattaforma si concretizzerebbe

in pregiudizi alla loro integrità personale e in danni morali, biologici e/o esistenziali nonché in svantaggi economici e sociali (discriminazioni per le condizioni di salute).
Gli effetti negativi sulle attività di diagnosi e cura, oltre che sulla ricerca scientifica e sui suoi esiti, potrebbe causare la perdita di chance per i malati e l'inefficacia delle terapie.
Nondimeno, sono state implementate misure specifiche, indicate e descritte nel precedente punto 3.3.3 e nella presente VIP, per contribuire a ridurre la gravità del rischio di modifiche indesiderate dei dati e i potenziali impatti negativi sugli Interessati.

3.4 PERDITA DI DATI

Se il rischio di perdita dei dati personali dovesse concretizzarsi, ci potrebbero essere impatti significativi sugli Interessati come di seguito riportati.
Gli Interessati potrebbero subire la perdita permanente delle proprie informazioni personali relative a dati sensibili come informazioni mediche e analisi cliniche; inoltre, l'intero progetto relativo alla ROC e alla sua Piattaforma sarebbe compromesso.
La perdita di dati potrebbe comportare conseguenze legali per la ROC e per i responsabili del trattamento dei dati.
Gli Interessati potrebbero intraprendere azioni legali per richiedere riparazioni o risarcimenti per il danno subito a seguito della perdita dei propri dati personali.
Gli Interessati potrebbero sperimentare disagio, preoccupazione e stress emotivo a causa della perdita dei propri dati personali.

3.4.1 Le principali minacce che potrebbero concretizzare il rischio.

Le principali minacce che potrebbero concretizzare il rischio di perdita di dati sono:

a) eventi come incendi, allagamenti, danni fisici ai dispositivi di archiviazione o guasti tecnici;
b) errori umani, come la cancellazione accidentale di dati, la sovrascrittura di file importanti o l'errata configurazione dei sistemi;
c) azioni illecite di hacker o di criminali informatici mirate alla Piattaforma e ai relativi asset;

d) operazioni di cracking delle credenziali di accesso;
e) utilizzo di tecniche di ingegneria sociale (furto di credenziali con mail) delle comunicazioni;
f) omissioni o errori nelle operazioni di backup o guasti ai sistemi di backup;
g) errori operativi in fase di ingresso e transito dei dati;
h) guasti dei sistemi di storage;
i) assenza di formazione specifica per gli incaricati coinvolti;
j) assenza di una policy specifica di gestione dei data breach;
k) assenza di controlli periodici e sistematici;
l) assenza di piani di recovery;
m) la perdita o il furto di asset e dispositivi di archiviazione che mette a rischio la sicurezza dei dati;
n) le vulnerabilità della Piattaforma e dei sistemi informativi;
o) le violazioni delle politiche di sicurezza o l'accesso non autorizzato ai dati da parte del personale

3.4.2 Le fonti di rischio.

Le fonti di rischio per la perdita dei dati possono derivare da diverse situazioni o fattori.

Alcune delle principali fonti di rischio includono:

a) la Piattaforma e le infrastrutture tecnologiche che ospitano e gestiscono i dati in quanto possono essere soggette a guasti, errori di configurazione o vulnerabilità di sicurezza che possono portare alla perdita dei dati;
b) i processi operativi all'interno delle organizzazioni dei titolari in quanto vulnerabili a errori umani, negligenze o mancanze di procedure adeguate, possono aumentare il rischio di perdita di dati;
c) le azioni o le negligenze umane che possono essere fonti significative di rischi per la perdita dei dati;

d) eventi naturali, come incendi, allagamenti, terremoti o furti, possono danneggiare l'infrastruttura logica o fisica in cui i dati sono conservati, portando alla loro perdita;
e) pur centralizzato il trattamento dei dati, la dipendenza da fornitori di servizi esterni per l'archiviazione, la gestione o il trattamento dei dati può comportare rischi, come la perdita dei dati a causa di violazioni della sicurezza o di errori da parte dei fornitori.

3.4.3 Le misure che contribuiscono a mitigare il rischio.

Per mitigare il rischio di perdite indesiderate dei dati, all'interno della ROC e della Piattaforma sono state adottate una serie di misure di sicurezza, anche descritte nei punti precedenti della presente DPIA

a) eseguire regolarmente backup e archiviazione dei dati utilizzando software specifici e aggiornati;
b) adottare e attuare politiche di disaster recovery e business continuità;
c) utilizzare la crittografia per proteggere i dati in transito;
d) implementare controlli di accesso e autenticazione per limitare l'accesso ai dati solo al personale autorizzato;
e) monitoraggio e rilevazione delle anomalie per identificare comportamenti sospetti o attività non autorizzate;
f) fornire una formazione adeguata al personale per sensibilizzarli sulla sicurezza dei dati;
g) eseguire regolarmente audit su eventuali responsabili esterni che trattano i dati;
h) stipulare contratti e accordi con fornitori esterni che gestiscono o trattano i dati.

3.4.4 Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate.

Le minacce individuate nei paragrafi precedenti devono essere valutate in base alla loro frequenza, alla loro complessità e alla loro capacità di superare le misure di sicurezza adottate. Considerando l'elevata probabilità di errori umani, di negligenza del personale,

di attacchi informatici nel settore dei dati sanitari o di eventi naturali, la probabilità del rischio è da considerarsi importante.
Nondimeno, le misure pianificate, come sopra descritte, contribuiscono a mitigare il rischio di modifiche indesiderate dei dati.

3.4.5 Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate.

La sensibilità dei dati trattati e il potenziale impatto sulle persone interessate rendono la gravità del rischio di perdita dei dati personali considerabile come importante in quanto potrebbe compromettere la validità e affidabilità della Piattaforma oltre ad arrecare gravi danni agli Interessati stessi che si vedrebbero privati di dati importanti relativi al proprio stato di salute come evidenziato nei paragrafi precedenti.
Tuttavia, sono state implementate misure specifiche (indicate e descritte nel precedente par. 3.4.3 e nella presente VIP) per contribuire a ridurre la gravità del rischio di perdita dei dati e i potenziali impatti negativi sugli Interessati.

4. CONCLUSIONI ED INDICAZIONI OPERATIVE.

Eseguita la valutazione d'impatto

- acquisito il parere del DPO e intervistati gli altri referenti coinvolti nelle attività di identificazione, analisi, valutazione e trattamento dei rischi, verificate le criticità sotto il profilo della gravità e della probabilità del verificarsi di minacce in merito alla protezione dei dati personali –

può ritenersi che:

- l'adozione delle misure tecniche ed organizzative individuate determini la mitigazione dei rischi entro limiti accettabili;
- sia garantito il rispertto dei principi di necessità e proporzionalità del trattamento.

In ragione di tutti i motivi esposti nel presente documento, le misure tecniche ed organizzative, ove adottate, aggiornate, costantemente monitorate, valutate e migliorate, consentono di definire accettabile il livello di rischio derivante dalle operazioni di trattamento effettuate

Il Titolare del trattamento

Istituto Nazionale Tumori IRCCS "Fondazione G.Pascale"

in persona del l.r.p.t.