GAMBIT

Raccolta di Evidenze dalla Pratica Clinica Reale sull'efficacia di Pembrolizumab nel Carcinoma Mammario Triplo Negativo in Stadio Precoce - Studio Gambit

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI – DPIA
ex art. 35 del Regolamento UE 2016/679, c.d. GDPR

Responsabili della redazione: Prof.ssa Maria Vittoria Dieci
Responsabile dell'approvazione: Prof. Umberto Cillo

Status: Validata 100%

INDICE

Nome del DPO/RPD	Dott. Giorgio Valandro
Posizione del DPO/RPD	È stata notificata la DPIA al DPO, ricevuto parere del DPO, il documento è stato integrato con le sue osservazioni.
Analisi del contesto	● Il consenso degli interessati verrà raccolto con un modulo cartaceo nella coorte prospettica. ● Non è stato possibile somministrare il consenso nella coorte retrospettiva poiché lo sforzo risulta sproporzionato. Vedesi Articolo 110 Codice della privacy (D.lgs. 30 giugno 2003, n. 196) ● Istituto Oncologico Veneto è accreditata come Istituti di Ricovero e Cura a Carattere Scientifico – IRCCS.

STUDIO DEL CONTESTO

PANORAMICA DEL TRATTAMENTO

Quale è il trattamento in considerazione?	Il trattamento ha ad oggetto i dati personali rientranti in particolari categorie: si tratta dei dati relativi alla salute raccolti mediante una revisione delle cartelle cliniche di reparto o di ambulatorio e dai documenti medici conservati nel dossier della persona, inclusi i dati amministrativi. La raccolta è finalizzata alla raccolta di evidenze dalla pratica clinica reale sull'efficacia del Pembrolizumab nel carcinoma mammario triplo negativo in stadio precoce. Il progetto prevede una fase retrospettiva e una fase prospettica. Questo studio osservazionale multicentrico retrospettivo-prospettico è stato progettato per valutare se i dati real-world confermano i benefici in termini di sopravvivenza globale osservati nello studio KEYNOTE-522 per i pazienti con tumore mammario triplo negativo in stadio precoce trattati con Pembrolizumab, l'arruolamento durerà fino al 01/04/2036. Coorti di trattamento: Lo studio includerà due coorti di pazienti con tumore mammario triplo negativo in stadio precoce sottoposti a chemioterapia sistemica neoadiuvante secondo la pratica clinica: • Gruppo Pembrolizumab: Pazienti trattati con Pembrolizumab in combinazione con chemioterapia neoadiuvante, seguita da trattamento adiuvante. • Gruppo di controllo: Pazienti trattati con sola chemioterapia neoadiuvante, con eventuale successivo trattamento adiuvante, senza Pembrolizumab. Verrà inoltre arruolato un terzo gruppo esploratorio: • Gruppo esploratorio (up-front surgery): Pazienti sottoposti a chirurgia primaria senza precedente trattamento neoadiuvante (gruppo adiuvante-only). L'obiettivo di arruolamento è di almeno 1.500 pazienti, di cui almeno 900 nei due gruppi principali trattati con terapia neoadiuvante. I pazienti saranno reclutati in almeno 26 Istituzioni italiane.
Criticità del trattamento:	L'esecuzione della DPIA per questo studio è stata ritenuta necessaria in ragione: - del volume e della tipologia di dati utilizzati (dati personali relativi alla salute); - dell'ampio numero e della tipologia d'interessati coinvolti (per lo più pazienti e, dunque, suscettibili di poter essere intesi quali soggetti vulnerabili); - della durata prolungata dell'attività di trattamento svolta nell'ambito del progetto;
Parere del DPO/RPD	La stima della probabilità del rischio porta a ritenere che lo studio, alla luce delle misure tecniche e organizzative attualmente in atto e, tenuto conto della natura del trattamento, possa essere implementato in futuro.
Quali sono le responsabilità connesse al trattamento?	TITOLARI AUTONOMI DEL TRATTAMENTO DEI DATI ● Promotore: **Università degli Studi di Padova - Dipartimento di Scienze Chirurgiche, Oncologiche e Gastroenterologiche (DiSCOG)** Contatti: - mail: ricercaclinica.discog@unipd.it - PEC: dipartimento.discog@pec.unipd.it - Numero di Telefono: 049821-2069/8832/2243

	● Centro coordinatore: **Istituto Oncologico Veneto-IRCCS**, legale rappresentante Dr.ssa Patrizia Simionato Contatti: - PEC: protocollo.iov@pecveneto.it - Numero di Telefono: 049/8215849 ● Responsabile scientifico (referente privacy): Prof.ssa Maria Vittoria Dieci, Principal Investigator dello studio. ● Data Protection Officer: Il Titolare si avvale di un Responsabile per la protezione dei dati personali (anche noto come Data Protection Officer "DPO") che vigila sulla conformità aziendale alla normativa a protezione dei dati personali. Il DPO può essere contattato tramite il seguente canale di comunicazione: - Il DPO nominato dall'Università di Padova (Dr. Giorgio Valandro) scrivendo una mail a: privacy@unipd.it - il DPO nominato dall'Istituto Oncologico Veneto-IRCCS scrivendo una mail a: rpd@iov.veneto.it. <u>Altri centri coinvolti nello studio e titolari autonomi del trattamento dei dati:</u> **Coordinating Center**: Istituto Oncologico Veneto IRCCS – Padova **Centri partecipanti (ordine alfabetico per città)** Clinica Oncologica Ospedali Riuniti di Ancona – Ancona Centro di Riferimento Oncologico (CRO) – Aviano ASST Papa Giovanni XXIII – Bergamo IOV Castelfranco Veneto – Castelfranco Veneto Humanitas Catania – Catania Ospedale di Cremona – ASST Cremona – Cremona Azienda Ospedaliero-Universitaria Careggi – Firenze Ospedale S. Martino – Genova Ospedale dell'Angelo – Mestre Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico – Milano Humanitas Milano – Milano Istituto Europeo di Oncologia – Milano Istituto Nazionale Tumori – Milano Ospedale San Raffaele IRCCS – Milano Azienda Ospedaliero-Universitaria di Modena – Modena Azienda Ospedaliera Napoli Federico II – Napoli Istituto Nazionale Tumori IRCCS Fondazione Pascale – Napoli Ospedale Maggiore – Novara Azienda Ospedaliero-Universitaria Pisana – Pisa Nuovo Ospedale di Prato Santo Stefano – Azienda USL Toscana Centro – Prato Azienda Ospedaliera Santa Maria Nuova – Reggio Emilia Policlinico A. Gemelli – Roma Policlinico Umberto I – Roma

	IRCCS Istituto Candiolo Centro Oncologico d'Eccellenza – Torino IRCCS Istituto Romagnolo per lo Studio dei Tumori "Dino Amadori" (IRST) - Designati del trattamento: tutte le persone fisiche che hanno accesso alle immagini, anche se non autorizzate a compiere alcuna operazione sulle stesse, sono designate incaricati del trattamento ("Designati"). La designazione degli Incaricati è effettuata per iscritto dal Titolare e individua puntualmente l'ambito del trattamento loro consentito. Ad esempio, nel caso specifico, accesso ai dati. Maria Vittoria Dieci Oncologia 2; Prof.ssa associata DiSCOG UNIPD. Gaia Griguolo Oncologia 2; Ricercatrice DiSCOG UNIPD Antonio Rosato Immunologia e Diagnostica Molecolare Oncologica; Prof. ordinario DiSCOG UNIPD ● Autorizzati al trattamento Tutte le persone fisiche che hanno accesso alle immagini, anche se non autorizzate a compiere alcuna operazione sulle stesse, sono designate del trattamento ("Autorizzati"). La designazione degli incaricati è effettuata per iscritto dal titolare e individua puntualmente l'ambito del trattamento loro consentito. Ad esempio, nel caso specifico, accesso ai dati. ● Prof.ssa Maria Vittoria Dieci, Oncologia 2, professoressa associata DiSCOG ● Prof. Antonio Rosato, Immunologia e Diagnostica Molecolare Oncologica, Professore Ordinario ● Dott. Davide Massa, dottorando DiSCOG ● Dott.ssa Stefania Lando, dottoranda DiSCOG di Statistica Medica ● Prof. Angelo Dei Tos, Anatomia Patologica, professore ordinario ● Prof. Stefano Piccolo, Dipartimento di Medicina Molecolare – Università di Padova: Studio delle proprietà fisiche e biologiche del tumore. ● Prof. Dario Gregori, Ordinario di Statistica Medica e responsabile dell'Unità di Biostatistica, Epidemiologia e Salute Pubblica presso il Dipartimento di Scienze Cardio-Toraco-Vascolari dell'Università di Padova. Soggetti nominati Responsabili del trattamento dei dati ex art. 28/GDPR: • Fondazione IRCCS Istituto Nazionale dei Tumori, Milano: Sequenziamento dell'RNA (RNA-seq) e analisi del profilo metabolico dei campioni. Supervisione: Dr. Claudio Vernieri. Il contratto di nomina a Responsabile del trattamento dei dati sarà subordinato all'effettiva stipula del contratto con INT per il sequenziamento dell'RNA. Al momento, tale contratto non risulta ancora formalizzato ma solo programmato.
Ci sono standard applicabili al trattamento?	Ancora in via del tutto generale, va ricordato che al trattamento "Sperimentazioni Cliniche" si applicano, tra le altre, le seguenti principali normative: • Regolamento UE n. 2016/679 (GDPR). - in particolare, art. 35 e 89 • D.lgs. n. 196/2003 ss.mm.ii per effetto del D.lgs. n. 101/2018

	- in particolare, art. 110 bis.1 e 110 bis.4 • Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica provv. n. 515/2018 del Garante per la protezione dei dati personali (Allegato A.5 del d.lgs. 196/2003 e ss.mm.ii.) • Provvedimento n. 146/2019 del Garante per la protezione dei dati personali recante le prescrizioni relative al trattamento di particolari categorie di dati - Prescrizioni relative al trattamento di dati personali effettuato per scopi di ricerca scientifica (Aut. Gen. n. 9/2016) • Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice (provvedimento n. 298/2024 del Garante) • DPR n. 439 del 21 settembre 2001 (sperimentazione clinica) • Legge n. 189 dell'8 novembre 2012 (sperimentazione clinica) • D.M. 27 aprile 2015 (sperimentazione clinica) • D.M. 30.11.2021 (natura no profit) • Determina AIFA del 20 Marzo 2008 (natura osservazionale)

DATI, PROCESSI E RISORSE DI SUPPORTO

Quali sono i dati trattati?	- Variabili demografiche: data di nascita, età alla diagnosi, peso, altezza, performance status (ECOG), data di morte (se applicabile). - Dettagli clinici e di trattamento: data della diagnosi, data dell'intervento chirurgico, stadiazione clinica e patologica (TNM, AJCC), referto patologico completo (tipo istologico, grado del tumore, Ki-67, ER, PR, HER2), densità dei linfociti infiltranti il tumore (TIL), stato mutazionale BRCA1/2, trattamenti oncologici (terapie sistemiche, radioterapia, chirurgia, ecc.), tipo di trattamento ricevuto (ad es, tipo di chemioterapia neoadiuvante, Pembrolizumab), dosaggio e durata del trattamento, tipo di procedura chirurgica. - Eventi avversi: incidenza di eventi avversi (secondo la classificazione CTCAE), gravità degli eventi avversi, gestione degli eventi avversi (interruzione del trattamento, riduzione della dose, ecc.). - Esito e follow-up: data della recidiva locale o sistemica (se applicabile), data della progressione della malattia (se applicabile), data dell'ultimo follow-up o del decesso, risposta al trattamento (ad esempio, pCR, risposta parziale con RCB) e progressione della malattia. Siti di recidiva metastatica (se applicabile). - condivisione slide digitalizzate dei campioni tumorali
Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?	Il Titolare del trattamento raccoglie i dati personali, anche di natura particolare, mediante revisione della cartella clinica e successivamente inseriti in Redcap. In caso di studio prospettico i dati saranno imputati direttamente in Redcap durante la visita di arruolamento; nella coorte retrospettiva i dati vengono aggiunti in Redcap copiandoli singolarmente dalla cartella clinica del paziente accessibile tramite E-Health. Nessun processo di export massivo di dati verrà implementato. Nella piattaforma di raccolta dati (Redcap) verranno inseriti solamente le variabili riportate nel punto soprastante. I dati saranno memorizzati in forma pseudonimizzata tramite un codice progressivo e non sarà possibile risalire all'identità e i soggetti senza avere accesso alla chiave di decodifica conservata separatamente. I dati raccolti non vengono diffusi e/o divulgati, ma vengono utilizzati per l'espletamento dello studio. Si applicano le disposizioni previste dalle Prescrizioni relative al trattamento di dati personali effettuato per scopi di ricerca scientifica (provvedimento n. 146/2019 del Garante per la protezione dei dati personali). La documentazione inerente alla sperimentazione sarà conservata per un periodo minimo di 7 anni (art. 18 del D.lgs. 200 del 6/11/2007) dopo il completamento della sperimentazione, ovvero per il tempo necessario all'assolvimento di ulteriori obblighi di legge. I dati raccolti saranno conservati per un periodo minimo di 15 anni dopo il completamento della sperimentazione. Alla fine del periodo di conservazione i dati verranno eliminati.
Quali sono le risorse di supporto ai dati?	Lo studio comporta la raccolta ed il trattamento dei dati personali di natura particolare, raccolti tramite l'utilizzo della cartella clinica su supporto elettronico. I software sono di seguito elencati: - E-Health/Galileo - applicazione Oncosys; - File excel crittografato in dismissione, tutti i dati verranno caricati nella nuova piattaforma di raccolta dati; - Redcap gestito da UBEP-UNIPD dall'approvazione dell'emendamento sottomesso il 9/03/2026.

PRINCIPI FONDAMENTALI

PROPORZIONALITA' E NECESSITA'

Gli scopi del trattamento sono specifici, espliciti e legittimi?	Gli scopi sono specifici, espliciti e legittimi, in quanto i dati personali di natura particolare sono raccolti e trattati esclusivamente per la conduzione dello studio, finalizzato alla raccolta di evidenze dalla pratica clinica reale sull'efficacia del Pembrolizumab nel carcinoma mammario triplo negativo in stadio precoce.
Quali sono le basi legali che rendono lecito il trattamento?	Base giuridica: <u>Studio prospettico</u>: consenso esplicito dell'interessato, ai sensi del combinato disposto tra l'art. 9, comma 2, lett. a) del GDPR e l'art. 7, comma 2, delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 <u>Studio retrospettivo</u>: ● consenso esplicito dell'interessato, ex art. 9, comma 2, lett. a) del GDPR ove possibile ● articolo 110 Codice della privacy (D.lgs. 30 giugno 2003, n. 196) quando lo sforzo risulta sproporzionato. Considerato che una parte significativa dei soggetti coinvolti nello studio è costituita da pazienti che interrompono il follow-up clinico e risultano non più raggiungibili tramite i recapiti disponibili, si procede preliminarmente a tentativi di contatto individuale utilizzando diversi canali: -email inviate agli indirizzi presenti nella documentazione clinica, che possono risultare inattivi o non consultabili: -contatti telefonici, laddove disponibili, che possono risultare dismessi o non raggiungibili. Nonostante questi sforzi, un numero rilevante di pazienti rimane irraggiungibile. Procedere a ulteriori tentativi comporta un onere organizzativo ed economico sproporzionato, tale da compromettere la sostenibilità e la prosecuzione della ricerca. Inoltre, si evidenzia la presenza di pazienti deceduti, per i quali non è previsto l'obbligo di informativa individuale. Il tentativo di contattare eventuali familiari o aventi causa comporterebbe un ulteriore onere organizzativo, economico ed etico sproporzionato e non giustificato ai sensi dell'art.110 del D.lgs 196/2003. Alla luce di quanto sopra, ai sensi del sopracitato articolo, si ritiene giustificato non procedere all'invio individuale dell'informativa a tali soggetti. Restano comunque garantite misure di tutela adeguate, nonché la pubblicizzazione per estratto della seguente DPIA e dell'informativa sul sito del Promotore e comunicazione al Garante per la protezione dei dati personali.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità dello studio. In particolare, le variabili selezionate sono definite in base a un protocollo approvato e rispondono a criteri di rilevanza scientifica e metodologica, evitando la raccolta di informazioni non essenziali o eccedenti. Non vengono acquisiti dati ulteriori rispetto a quelli indispensabili per le analisi statistiche previste, e tutti i campi informativi superflui o non strettamente legati agli obiettivi primari dello studio vengono omessi in fase di raccolta o anonimizzati/pseudonimizzati in fase di gestione. Tale approccio garantisce la piena aderenza al principio di minimizzazione dei dati previsto dall'art. 5 del GDPR, oltre a ridurre i rischi per i diritti e le libertà fondamentali degli interessati.
I dati sono esatti e aggiornati?	I dati sono esatti ed aggiornati e sono basati sulla disponibilità degli stessi nelle cartelle cliniche aziendali.
Qual è il periodo di conservazione dei dati?	La documentazione inerente alla Sperimentazione sarà conservata per un periodo minimo di 7 anni (art. 18 del D.lgs. 200 del 6/11/2007) dopo il completamento della sperimentazione, ovvero per il tempo necessario all'assolvimento di ulteriori obblighi di legge. I dati personali vengono conservati per un periodo minimo di 15 anni dal termine del trattamento principale, al fine di garantire la completezza del follow-up clinico, consentire eventuali verifiche successive, assicurare la riproducibilità dei risultati scientifici e gestire eventuali richieste di chiarimento o contenziosi. Trascorso tale periodo minimo, i dati sono ulteriormente conservati solo per il tempo strettamente necessario al completamento delle analisi statistiche e scientifiche, in conformità con i principi di limitazione della conservazione (art. 5, par. 1, lett. e) del GDPR).

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Come sono informati del trattamento gli interessati? **Ove applicabile: come si ottiene il consenso degli interessati?**	Gli interessati al trattamento sono informati tramite le seguenti modalità: a) fase PROSPETTICA: - tramite informativa estesa redatta ai sensi dell'articolo 13 del GDPR, che viene fatta sottoscrivere ai soggetti partecipanti per presa visione e il consenso viene fatto firmare in fase di visita. b) fase RETROSPETTIVA: Trattandosi di pazienti oncologici nella coorte retrospettiva, con un alto tasso di mortalità, lo sforzo per raggiungere gli stessi o eventualmente i parenti in caso di decesso è ritenuto sproporzionato. Considerato che una parte significativa dei soggetti coinvolti nello studio è costituita da pazienti che interrompono il follow-up clinico e risultano non più raggiungibili tramite i recapiti disponibili, si procede preliminarmente a tentativi di contatto individuale utilizzando diversi canali: · Email inviate agli indirizzi presenti nella documentazione clinica, che possono risultare inattivi o non consultati; · Contatti telefonici, laddove disponibili, che possono risultare dismessi o non raggiungibili Nonostante questi sforzi, un numero rilevante di pazienti rimane irraggiungibile. Procedere a ulteriori tentativi comporta un onere organizzativo ed economico sproporzionato, tale da compromettere la sostenibilità e la prosecuzione della ricerca. Inoltre, si evidenzia la presenza di pazienti deceduti, per i quali non è previsto l'obbligo di informativa individuale. Il tentativo di contattare eventuali familiari o aventi causa comporterebbe un ulteriore onere organizzativo, economico ed etico sproporzionato, potenzialmente invasivo e non giustificato ai sensi dell'art. 110 del D.lgs. 196/2003. Alla luce di quanto sopra, ai sensi dell'art. 110 del D.lgs. 196/2003, si ritiene giustificato non procedere all'invio individuale dell'informativa a tali soggetti. Restano comunque garantite misure di tutela adeguate, nonché la pubblicazione per estratto della presente DPIA sul sito istituzionale del Promotore e la comunicazione al Garante per la protezione dei dati personali. Il tempo necessario per l'aggiornamento del consenso per questa casistica rischia così di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca come riportato nell'articolo 110 Codice della privacy 30 giugno 2003, n. 196 dato. L'informativa privacy è consultabile sul sito web www.discog.unipd.it Il Promotore, in ogni caso, renderà pubblico un estratto della presente valutazione d'impatto attraverso il proprio sito web istituzionale e la relativa informativa in modo da rendere comunque conoscibile e trasparente il presente trattamento di dati personali. Il Promotore, in ogni caso, in base a quanto previsto dal Provv. n. 298/2024 del Garante, l'estratto della DPIA pubblicherà in una pagina del sito istituzionale del Dipartimento e comunicherà al Garante per la protezione dei dati personali.
Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?	L'interessato può in qualsiasi momento esercitare i diritti di cui agli artt. 15-22 GDPR, scrivendo a mail: ricerca.discog@unipd.it; PEC: dipartimento.discog@pec.unipd.it Policy aziendali per la gestione delle richieste da parte degli interessati: https://www.unipd.it/sites/unipd.it/files/2021/Delibera21.07.2020.Rep_.202-Prot.347215.pdf

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?	L'interessato può in qualsiasi momento esercitare i diritti di cui agli artt. 15-22 GDPR, scrivendo una mail/PEC: - ricerca.discog@unipd.it - dipartimento.discog@pec.unipd.it Diritto di chiedere, ai riferimenti riportati di seguito, di accedere ai propri dati personali e di rettificarli se inesatti, di cancellarli o limitarne il trattamento se ne ricorrono i presupposti, di opporsi al loro trattamento per legittimi interessi perseguiti dal Titolare, nonché di ottenere la portabilità dei dati personalmente forniti solo se oggetto di un trattamento automatizzato basato sul consenso o sul contratto. Diritto di revocare il consenso prestato per le finalità di trattamento che lo richiedono, ferma restando la liceità del trattamento effettuato sino al momento della revoca. Modulo disponibile al link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924 con successivo inoltro ai riferimenti forniti.
Gli obblighi degli autorizzati al trattamento sono definiti con chiarezza e disciplinati da un contratto?	Le istruzioni per gli autorizzati al trattamento dei dati sono le istruzioni generali di Ateneo e sono pubblicate al seguente link: https://www.unipd.it/privacy
In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?	Non è attualmente previsto alcun trasferimento di dati verso Paesi al di fuori dello Spazio Economico Europeo (SEE); qualora intervenissero modifiche in tal senso, la DPIA sarà tempestivamente aggiornata. Il promotore potrà ricevere dati provenienti da strutture al di fuori dell'Italia e dell'Unione Europea esclusivamente in forma anonima e aggregata, e pertanto non riconducibili a persone fisiche identificate o identificabili e pertanto non soggetti all'applicazione del GDPR.

RISCHI

MISURE ESISTENTI O PIANIFICATE (Redcap)

Controllo degli accessi logici	Controllo degli accessi logici RedCap implementa un sistema di ruoli e permessi che consente agli amministratori di definire in modo granulare chi può accedere a determinati dati e funzionalità. Gli utenti vengono assegnati a ruoli specifici con privilegi limitati in base alle loro necessità operative. Gli accessi sono controllati tramite: - Credenziali: nome utente generato dall'UBEP e password impostata dall'utente nel rispetto di criteri di complessità (secondo le regole di Microsoft Authenticator) - Doppia Autenticazione con Microsoft Authenticator: verifica in due passaggi con invio di una password temporanea utilizzabile una sola volta tramite Microsoft Authenticator installato nel proprio dispositivo mobile.
Tracciabilità	Redcap mantiene un registro dettagliato delle attività degli utenti, compreso l'accesso ai dati, la modifica di dati o configurazioni, e i tentativi falliti di accesso. Questo consente una piena tracciabilità delle azioni compiute nel sistema e facilita l'individuazione di attività sospette o non autorizzate. Le applicazioni e le macchine in uso al gestore sono dotate di registri delle attività.
Minimizzazione dei dati	Il protocollo condiviso e autorizzato con il Comitato Etico stabilisce sia il set di informazioni cui si può accedere, sia o il dataset di informazioni che devono essere poi successivamente raccolte, catalogate e valutate, oltre anche all'arco temporale di analisi. L'accesso ai dati clinici è consentito solamente al personale medico, mentre al restante personale (ricercatori), è consentito il trattamento dei soli dati necessari all'attività di ricerca prevista dal singolo progetto.
Sicurezza dei siti web	Il sistema operativo è aggiornato all'ultima versione disponibile e vengono regolarmente applicate le eventuali patch software di sicurezza. Il sistema è protetto da firewall e da software antivirus.
Backup	Backup regolari: il sistema in oggetto implementa backup automatici periodici per garantire che i dati possano essere ripristinati in caso di perdita o danneggiamento. Questi backup sono conservati su server separati o in posizioni fisicamente distinte, riducendo il rischio di perdita di dati causata da problemi hardware, software o disastri naturali.
Session timeout (REDCap)	Le sessioni utente vengono automaticamente terminate dopo un periodo di inattività predefinito di 30 minuti, per prevenire accessi non autorizzati ai dati lasciati esposti.
Politica di tutela della privacy	Rispetto della normativa europea ed italiana vigente in ambito Privacy e rispetto delle istruzioni agli incaricati privacy UniPD: https://drive.google.com/file/d/1p11RPbNeOUR_lyfLYP7K1pM1QeefGciD/view Procedura per la gestione delle violazioni di dati personali (data breach): https://www.unipd.it/sites/unipd.it/files/2021/Procedura%20data%20breach_0.pdf
Pseudonimizzazione	La pseudonimizzazione in REDCap è un processo che separa i dati identificativi dei partecipanti alla ricerca dai dati della ricerca stessa, sostituendoli con identificatori univoci (pseudonimi). In concreto:

	- Viene assegnato un "Record ID" univoco a ogni partecipante - Il Record ID sostituisce i dati identificativi diretti in tutto il sistema I dati personali inseriti nella piattaforma sono sottoposti a procedura di pseudonimizzazione rendendo di fatto impossibile la reidentificazione degli interessati nel caso di data breach della sola piattoforma Redcap
Password	La password deve essere cambiata ogni tre mesi, per impostazione le ultime 5 password non possono essere riutilizzate.
Crittografia	RedCap si basa su protocolli HTTPS(HyperText Transfer Protocol Secure) un'estensione del protocollo HTTP, progettato per garantire comunicazioni sicure su Internet. Utilizza la crittografia per proteggere i dati scambiati tra il client (tipicamente un browser web) e il server, impedendo così a terzi non autorizzati di intercettare o manomettere le informazioni.
Controllo degli accessi fisici	L'accesso ai locali è bloccato da serrature con codice: il codice di accesso è rilasciato al solo personale che abbia necessità ad accedere a tali locali (anche se condivisi con altri professionisti), oltre al personale del servizio di pulizia.
Vigilanza sulla protezione dei dati	Il promotore ha adottato un organigramma privacy e rivede con cadenza periodico le procedure e le documentazioni prodotte in ossequio al Regolamento (UE) 679/2016.
Integrare la protezione della privacy nei progetti	Il promotore, conformemente alla disciplina del Reg. (UE) 2016/679, gestisce i dati nel rispetto del principio di privacy per impostazione predefinita e per disegno. I dati trattati sono soltanto quelli strettamente necessari per le finalità perseguite, in ossequio al principio di minimizzazione.

ACCESSO ILLEGITTIMO AI DATI (Redcap)

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	Perdita di riservatezza e perdita di controllo sull'utilizzo dei dati. La diffusione del dato può comportare elevati rischi all'interessato. In linea generale la perdita di riservatezza determinerebbe la mancanza di controllo sull'utilizzo degli stessi, con impatti tanto materiali quanto immateriali significativi, vista anche la categoria particolarmente vulnerabile di interessati coinvolti nel trattamento.
Quali sono le principali minacce che potrebbero concretizzare il rischio?	Sottrazione delle credenziali di accesso, attacco al sistema informativo che sfrutti eventuali vulnerabilità della piattaforma non ancora segnalate/corrette.
Quali sono le fonti di rischio?	Esposizione ad internet della piattaforma che la espone agli attacchi esterni. Comportamento improprio personale interno, comportamento improprio personale esterno, hacker.
Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	Controllo degli accessi logici, Session timeout (REDCap), Tracciabilità, Lotta contro il malware, Crittografia, Minimizzazione dei dati, Gestione dei privilegi di accesso (Profilazione) secondo principio "minima autorizzazione richiesta", Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Password, Prevenzione delle fonti di rischio, Vigilanza sulla protezione dei dati
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	Limitato, per quanto concerne la loro gestione attraverso la piattaforma RedCap, in quanto vi sono memorizzati esclusivamente dati già pseudonimizzati. Il processo di identificazione sarebbe possibile solo con un ulteriore accesso al file di decrittazione conservato off-line in un dispositivo protetto da password e conservato in luogo accessibile fisicamente solo al promotore. Si raccomanda in ogni caso di porre molta attenzione al processo di pseudonimizzazione, alla vigilanza sulla protezione dei dati personali, alla sicurezza dei canali informatici e alla formazione del personale in modo da ridurre ulteriormente il rischio ma anche gli effetti lesivi di un eventuale accesso illegittimo.
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	Limitata, date le misure di minimizzazione, di pseudonimizzazione, backup, controllo degli accessi logici, di sicurezza dei canali informatici, cifratura, password forte, archiviazione, formazione del personale, gestione dei terzi che accedono ai dati, nonché dalle misure di sicurezza impiegate dal promotore e attestate dalla DPIA acquisita dall'Istituto il rischio di eventuale accesso illegittimo dei dati residuale rimane limitata.

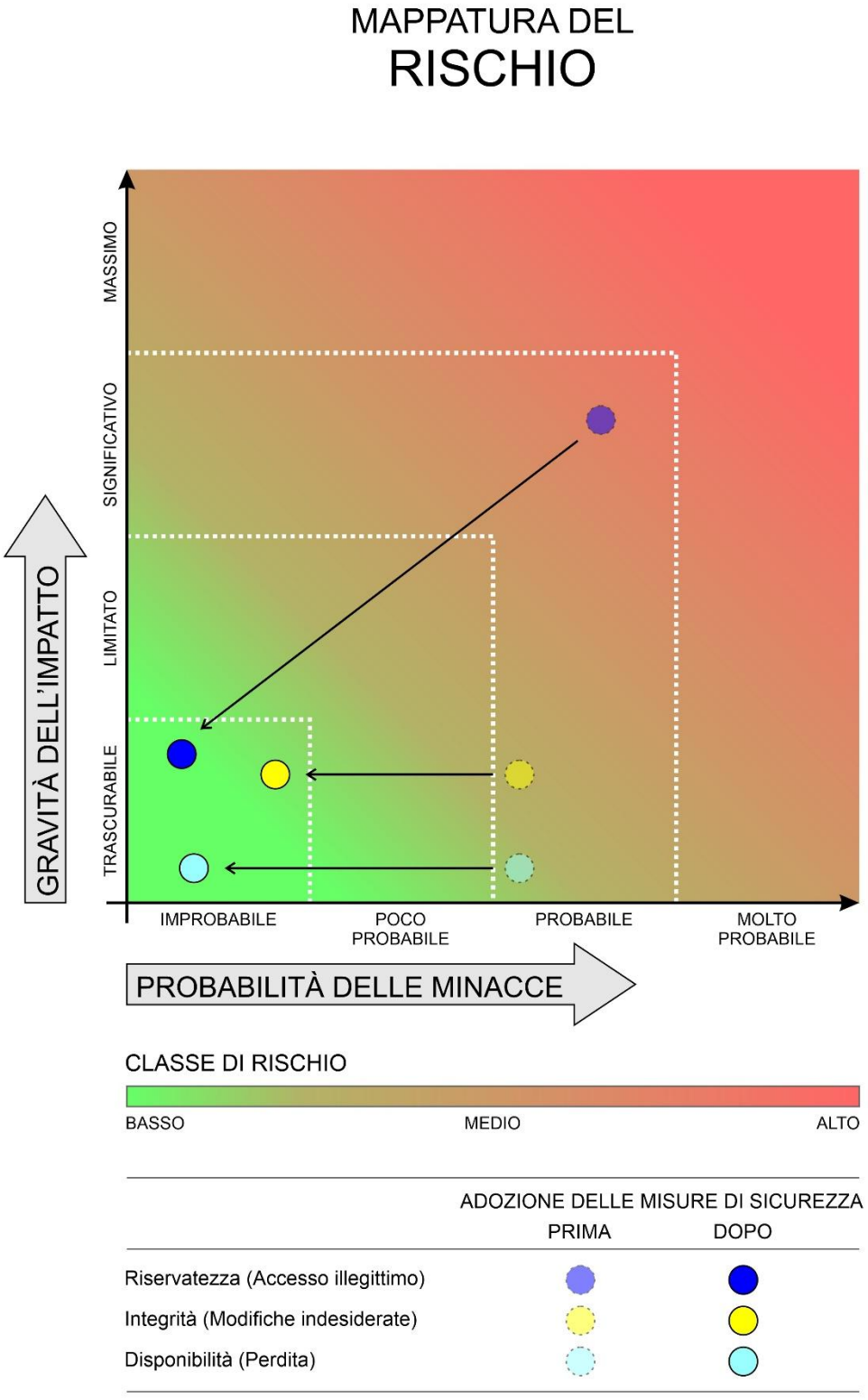
MODIFICHE INDESIDERATE DEI DATI (Redcap)

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?	Nessun impatto reale, I dati possono essere agevolmente re-inseriti a partire dalle cartelle cliniche.
Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?	Attacco dal WEB che sfrutti eventuali vulnerabilità della piattaforma non ancora segnalate/corrette. Il software è accessibile dalla rete. Comportamento improprio personale interno, comportamento improprio personale esterno.
Quali sono le fonti di rischio?	Esposizione ad internet della piattaforma che la espone agli attacchi esterni e/o un errore materiale
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	Controllo degli accessi logici, Tracciabilità, Sicurezza dei siti web, Backup, Politica di tutela della privacy
Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?	Trascurabile, i dati raccolti tramite il software RedCap sono protetti da idonee misure di sicurezza predisposte, volte a prevenire o ridurre al minimo i rischi di accesso non autorizzato o trattamento non consentito o non conforme alle finalità per cui i dati sono stati raccolti. Nessun impatto reale sui diritti e le libertà degli interessati la modifica dei dati dello studio ha un impatto esclusivamente sui risultati dello studio.
Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?	Trascurabile, poiché il personale altamente specializzato e motivato. A fronte delle robuste misure di sicurezza implementate, si ritiene poco probabile l'evento di accesso illegittimo da parte di soggetti non autorizzati. I dati in ogni caso possono essere facilmente ripristinati grazie alle politiche di backup.

PERDITA DI DATI (Redcap)

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?	Rallentamento dello studio. Nessun impatto sugli interessati, i dati possono essere agevolmente re-inseriti a partire dalle cartelle cliniche
Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?	Attacco dal WEB che sfrutti eventuali vulnerabilità della piattaforma non ancora segnalate/corrette. Il software è accessibile da internet. Guasto hardware che potrebbe temporaneamente compromette l'accesso alla piattaforma RedCap. Furto dei server che ospitano la piattaforma RedCap.
Quali sono le fonti di rischio?	Accessibilità tramite la rete internet della piattaforma che la espone agli attacchi esterni. Vulnerabilità legata alle caratteristiche dell'hardware. Comportamento improprio personale interno/esterno, disastro naturale, malfunzionamento tecnico. Non rispetto delle buone prassi in caso di smaltimento dei supporti di memoria a seguito di sostituzione.
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	Lotta contro il malware, gestione dei privilegi di accesso secondo principio "minima autorizzazione richiesta", backup. Accesso controllato alla sala serve. Distruzione dei dispositivi di memoria a seguito di smaltimento.
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	Trascurabile, perché i dati raccolti tramite il software RedCap sono protetti da idonee misure di sicurezza predisposte, volte a prevenire o ridurre al minimo i rischi di perdita degli stessi grazie a una corretta politica di backup e perché i dati possono essere agevolmente re-inseriti a partire dalle cartelle cliniche In ogni la perdita dei dati comporterebbe solo un rallentamento dello studio in oggetto.
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	Improbabile, viste le misure applicate, quali quelle di archiviazione, di sicurezza dei canali informatici e delle politiche di gestione degli incidenti di sicurezza. La probabilità che ciò si realizzi risulta limitata anche se si raccomanda di porre molta attenzione alla formazione e gestione del personale, all'implementazione della politica dei backup e delle politiche della privacy in generale.

PANORAMICA DEI RISCHI



CONVALIDA

Convalida
Io sottoscritto [nome e cognome del Direttore del Dipartimento di Scienze Chirurgiche Oncologiche e Gastroenterologiche (DiSCOG) delegato privacy dell'Università degli Studi di Padova, dopo aver esaminato la Valutazione d'impatto e la documentazione allegata, dichiaro:

1. che la descrizione del contesto del trattamento è aderente alla realtà;
2. che la descrizione dei rischi individuati è aderente alla realtà;
3. di ritenere appropriato il livello di rischio stimato sulla base delle misure esistenti e pianificate;
4. di autorizzare l'adozione delle misure di sicurezza individuate nel piano d'azione.

Direttore del Dipartimento DISCOG

Prof. Umberto Cillo

Nome del DPO/RPD
DPO UNIPD Dott. Giorgio Valandro

Posizione del DPO/RPD
-

Parere del DPO/RPD
La DPIA revisionata deve essere "validata" e sottoscritta dal Direttore del dipartimento, che è delegato privacy in base all'Organigramma privacy dell'Ateneo.

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
È stata chiesta la valutazione preventiva da parte del Comitato Etico Territoriale.