SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

OECI COMPREHENSIVE Cancer Centre

VALUTAZIONE D'IMPATTO PER PROGETTI DI RICERCA IN AMBITO SANITARIO

SU DATI RETROSPETTIVI

(ART. 110 D. LGS. 196/2003, Provvedimento Garante n. 146/2009)

La valutazione di impatto (DPIA) consente di identificare in modo puntuale i rischi per la protezione dei dati personali quando vengono pianificati nuovi progetti di ricerca o aggiornati progetti di ricerca in corso e di individuare le azioni necessarie per mitigare tali rischi.

Una valutazione di impatto, secondo l'Autorità Garante per la protezione dei dati personali, deve sempre essere effettuata negli studi retrospettivi quando:

- il trattamento dei dati personali è su larga scala;
- vengono trattate categorie particolari di dati, ad esempio dati genetici;
- l'attività comporta il data linkage di molteplici e diversi archivi di dati;
- l'attività prevede la rilevazione di dati per individui vulnerabili (minori, soggetti con patologie psichiatriche, anziani, ecc.);
- la base giuridica per il trattamento dei dati non è riferibile al consenso al trattamento, a ricerche condotte sulla base di disposizioni di legge o regolamento o al diritto, o ad altre specifiche fattispecie previste dal GDPR e dal Codice Privacy.

A CURA DEL RICERCATORE

Titolo dello studio: Protocollo di Real-life italiana per la descrizione degli Outcome in pazienti affetti carcinoma del polmone a piccole cellule (SCLC) trattati con chemio-ImmunoTerapia con inibitori del checkpoint immunitario

Codice di Protocollo: PROSIT

Titolare/i del trattamento: Azienda U.S.L. – IRCCS di Reggio Emilia e Università di Bologna - Alma Mater Studiorum

Principal Investigator: Dr.ssa Francesca Zanelli

S.C./S.S.D./Unità Oncologia Medica Provinciale

Data compilazione 18/11/2024

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

OECI COMPREHENSIVE Cancer Centre

TRATTAMENTO DEI DATI	
Descrizione del trattamento *(compilare i campi successivi o allegare il modulo di fattibilità dello studio)*	
Sinossi dello Studio	Studio osservazionale di coorte con una fase retrospettiva ed una fase prospettica. **Criteri di inclusione** • Età ≥18 anni. • Diagnosi cito-istologica di SCLC in stadio avanzato (recidiva non operabile, malattia avanzata o metastatica). In caso di SCLC, saranno inclusi anche i pazienti con malattia limitata (LD), come definita dalla stadiazione tumorale secondo VALG revisionata dalla IASLC • Trattamento con un ICI in combinazione con chemioterapia a base di platino (carboplatino o cisplatino) ed etoposide (fase retrospettiva) o candidabili a tale trattamento secondo le indicazioni riportate in scheda tecnica (fase prospettica) oppure trattamento con un inibitore del checkpoint immunitario dopo radiochemioterapia concomitante (fase retrospettiva) o candidabili a tale trattamento secondo le indicazioni riportate in scheda tecnica (fase prospettica) • Ottenimento del consenso informato. **Criteri di esclusione** • Nessuno **Obiettivo primario** • Descrivere l'efficacia ("effectiveness") della chemioimmunoterapia con atezolizumab o durvalumab, in combinazione con carboplatino o cisplatino ed etoposide in pazienti affetti da ES-SCLC come da indicazioni in scheda tecnica dei farmaci nel setting della comune pratica clinica in Italia **Obiettivi secondari** • Valutare la sicurezza della chemio-immunoterapia con atezolizumab o durvalumab, in combinazione con carboplatino o cisplatino ed etoposide in pazienti affetti da ES-SCLC come da indicazioni in scheda tecnica dei farmaci nel setting della comune pratica clinica in Italia • Valutare la sicurezza e l'impatto sull'outcome della RTE in pazienti affetti da ES-SCLC e trattati con atezolizumab o durvalumab, in combinazione con chemioterapia a base di platino (carboplatino o cisplatino) ed etoposide nel setting della comune pratica clinica in Italia

	• Valutare la sicurezza e l'impatto sull'outcome della PCI in pazienti affetti da ES-SCLC e trattati con atezolizumab o durvalumab, in combinazione con chemioterapia a base di platino (carboplatino o cisplatino) ed etoposide nel setting della comune pratica clinica in Italia • Descrivere la popolazione di pazienti affetti da ES-SCLC che accede alla seconda linea di terapia, e l'attività e l'efficacia delle terapie di seconda linea in pazienti affetti da ES-SCLC che progrediscono alla prima linea di chemio-immunoterapia nel setting della comune pratica clinica in Italia • Valutare l'impatto dell'abitudine tabagica e sue variazioni sugli outcome della chemio-immunoterapia con atezolizumab o durvalumab, in combinazione con carboplatino o cisplatino ed etoposide in pazienti affetti da ES-SCLC come da indicazioni in scheda tecnica dei farmaci nel setting della comune pratica clinica in Italia • Valutare l'efficacia e la sicurezza dell'immunoterapia di mantenimento dopo chemioradioterapia concomitante in pazienti affetti da SCLC **Endpoint primario:** sopravvivenza globale (OS), misurata dalla data di diagnosi alla data di decesso per qualsiasi causa. **Endpoints secondari:** o Frequenza e gravità degli eventi avversi classificati secondo il Common Terminology Criteria for Adverse Events (CTCAE) v5.0 in pazienti affetti da ES-SCLC e trattati con atezolizumab o durvalumab, in combinazione con chemioterapia a base di platino (carboplatino o cisplatino) ed etoposide; o Sopravvivenza libera da progressione (PFS) misurata dalla data di inizio della chemio-immunoterapia di prima linea alla data di progressione radiologica di malattia o di decesso per qualsiasi causa, qualunque avvenga prima; o Tasso di risposta radiologica globale (ORR), secondo criteri RECIST v 1.1 [ref] definito come la somma dei pazienti che presentano risposte parziali (PR) e complete (CR) dopo la terapia sul totale dei pazienti che hanno ricevuto almeno un ciclo di terapia; o Frequenza di effetti collaterali di grado ≥3 secondo il CTCAE v 5.0 in corso e dopo RTE, con particolare riferimento alla frequenza di polmoniti o PFS ed OS calcolate nel sottogruppo dei pazienti affetti da ES-SCLC che hanno ricevuto RTE sul residuo toracico in risposta dopo atezolizumab o durvalumab, in combinazione con chemioterapia a base di platino (carboplatino o cisplatino) ed etoposide

	o PFS ed OS calcolate nel sottogruppo dei pazienti affetti da ES-SCLC che hanno ricevuto PCI in assenza di progressione ad atezolizumab o durvalumab in combinazione con chemioterapia a base di platino (carboplatino o cisplatino) ed etoposide o ORR, PFS e OS misurate dall'inizio della seconda linea di trattamento, in maniera globale e differenziata per tipo di trattamento. o ORR, PFS, e OS tra gruppi in sottogruppi definiti da a storia di fumo, modifiche dell'abitudine tabagica dall'inizio dell'immunoterapia, e tipo di prodotto del tabacco utilizzato o ORR, PFS, OS, e numero e gravità degli eventi avversi dei pazienti che ricevono immunoterapia di mantenimento dopo radiochemioterapia concomitante per SCLC **Trattamento:** L'adesione al presente studio non modifica la normale pratica clinica e gli specifici interventi terapeutici saranno condotti con le medesime modalità e tempistiche che sarebbero adottati in assenza del presente protocollo di ricerca e secondo quanto riportato in Scheda Tecnica. **Dimensione del campione** Le dimensioni del campione non sono prevedibili a priori, in quanto dipenderanno dal numero di centri partecipanti e dal volume dei singoli centri. In base all'incidenza della patologia ed ai criteri di eleggibilità dello studio, ci aspettiamo circa 200 pazienti inseriti per la fase retrospettiva (di cui circa 20 dal centro coordinatore) e circa 200 pazienti per la fase prospettica (di cui circa 20 dal centro coordinatore) da 30 centri italiani. **Durata dello studio** - Data inizio studio: dopo approvazione del CE e rilascio del Nulla Osta da parte della Direzione Generale - Data raccolta dati/inizio arruolamento: dopo approvazione del CE e rilascio del Nulla Osta da parte della Direzione Generale - Periodo retrospettivo considerato per la raccolta dati: dal 1° gennaio 2015 al 30/09/2024 - Periodo prospettico: 4 anni - Durata complessiva dello studio: 5 anni (di cui 1 anno di follow-up)
Tipologia di dati raccolti	

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

OECI COMPREHENSIVE Cancer Centre

Modalità di raccolta *(fonte dei dati) (barrare anche più caselle)*	X da cartelle cliniche/documentazione sanitaria X da archivi di dati clinici (esempio Dossier Sanitario - DWH) ☐ da archivi di test diagnostici ☐ da dati di laboratorio ☐ da database amministrativi ☐ altro (specificare) _____
Trattamento dei dati *(indicare il supporto utilizzato per la rilevazione e conservazione dei dati)*	☐ In formato cartaceo X In formato digitale ☐ altro (specificare) _____
Categorie di persone interessate	X pazienti ☐ persone sane ☐ operatori sanitari ☐ *altro (specificare)* _____
Categorie di dati trattati	X dati sulla salute fisica o psichica ☐ dati genetici ☐ informazioni sulla vita sessuale ☐ informazioni sull'orientamento sessuale ☐ informazioni sugli stili di vita e/o le condizioni socioeconomiche ☐ informazioni su istruzione e formazione professionale ☐ anamnesi lavorativa ☐ informazioni su religione o altre credenze ☐ *altro (specificare)*
I dati personali (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati/condivisi con altri?	☐ No X Sì Se sì, selezionare uno o più ambiti di comunicazione: X Promotore CRO
I dati personali (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono trasferiti all'estero?	X No Sì Se sì Paesi area UE Paesi extra UE In quale/i Paese/i all'interno dell'area o extra UE
Misure di protezione dei dati	

Verranno conservati i dati identificativi dei partecipanti?	No X Sì Se sì, specificare le ragioni sottese a tale esigenza: Il Centro Partecipante conserverà i dati personali dell'Interessato (identificati esclusivamente tramite il Codice Univoco) per un periodo di 7 anni.
Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca	Per non identificare direttamente l'interessato sono adottate le seguenti misure: ☐ Adozione di tecniche crittografiche X Utilizzo di codici univoci per ciascun partecipante. Solo il responsabile della ricerca o altri soggetti autorizzati, possono (con l'uso di mezzi ragionevoli) collegare i codici all'identità dei partecipanti Il Promotore tratterà i dati dell'Interessato, in modo che siano privati degli elementi identificativi (ad esempio del nome e cognome), con l'effetto che il Promotore non conoscerà l'identità dell'Interessato. Tale processo (detto processo di "pseudonimizzazione") è svolto a cura del Centro di Sperimentazione e consiste nell'attribuzione ai dati dell'Interessato di un elemento univoco (ad esempio un numero o un codice alfanumerico). L'associazione tra tale codice (d'ora in poi definito "Codice Univoco") e i dati identificativi dell'Interessato è conservata esclusivamente dallo Sperimentatore Principale e da eventuali suoi collaboratori in modo sicuro e confidenziale. Le informazioni raccolte nell'ambito dello studio sono quindi condivise tra il Centro di Sperimentazione e il Promotore nell'ambito dello studio in oggetto, nonché nelle comunicazioni ad esso relative, solo in forma pseudonimizzata ☐ Altro, specificare _____ Per anonimizzare o aggregare i dati, anche in un momento successivo alla raccolta, sono adottate le seguenti misure: ☐ I dati personali, a seguito della raccolta sono eliminati definitivamente senza la possibilità di risalire ai dati originali ☐ I dati personali sono sostituti da uno o più identificatori, che possono essere utilizzati per un set di dati o per ogni singolo dato con distruzione del dato personale originario ☐ Sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati ☐ Altro (specificare) _____

PRINCIPI, FINALITA' E BASI GIURIDICHE
Necessità e proporzionalità

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

OECI COMPREHENSIVE Cancer Centre

Sono trattati solo i dati necessari e pertinenti al perseguimento delle finalità della ricerca (Minimizzazione)?	X Sì ☐ No Se no, specificare i motivi e le azioni previste _____ _____ _____ _____
Integrità ed esattezza	
Sono state messe in campo azioni per garantire l'integrità ed esattezza dei dati?	X Sì ☐ No Se no, specificare i motivi e le azioni previste _____ _____
Limitazione della conservazione	
Per quanto tempo verranno conservati i dati raccolti?	Indicare il numero di 7 anni Decorso tale termine i dati verranno: ☐ Anonimizzati completamente ☐ Distrutti X altro (*specificare*): Considerato che nuove scoperte potrebbero indicare inedite opportunità di indagine ai ricercatori o consentire di effettuare ulteriori studi e ricerche sui dati personali appartenenti a categorie particolari per lo studio di cui trattasi, l'Interessato può, liberamente e facoltativamente, acconsentire alla conservazione prolungata dei dati di cui al punto (A) da parte: ☐ del Centro di Sperimentazione per un periodo di… anni dalla conclusione del presente studio e/o ☐ dell'Alma Mater Studiorum – Università di Bologna, anche in forma identificativa, per un periodo di 15 anni dalla conclusione del presente studio per essere ricontattato affinché possa esprimere, se lo riterrà, un nuovo specifico consenso e autorizzare così una nuova ricerca sui propri dati per finalità differenti da quelle qui descritte. Ove invece l'Interessato neghi il consenso al trattamento qui descritto, i dati verranno cancellati ovvero resi anonimi immediatamente allo scadere dei termini di conservazione indicati al punto.
Basi giuridiche	

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

OECI COMPREHENSIVE Cancer Centre

Quali sono le basi giuridiche del trattamento?	☐ art. 9, par. 2, lett. j) GDPR[1] ☐ art. 110, co. 1 primo periodo Codice Privacy[2] **X** art. 110, co. 1, secondo periodo Codice Privacy[3]

MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO	
Informativa e consenso	
SOLO SE LA BASE GIURIDICA È L'ART. 110, CO. 1, SECONDO PERIODO Indicare i motivi per i quali non è possibile fornire l'informativa ai partecipanti allo Studio (soggetti interessati) e acquisirne il consenso	☐ motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione X sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati in ragione: o del numero molto alto di interessati che è stato stimato X deceduti o non contattabili
Nel caso di studi retrospettivi su dati genetici, ove non sia possibile ottenere il consenso informato, indicare se ricorrono le condizioni indicate	☐ indagini statistiche o ricerche scientifiche previste dal diritto dell'Unione europea, dalla legge o, nei casi previsti dalla legge, da regolamento ☐ scopi scientifici e statistici direttamente collegati con quelli per i quali è stato originariamente acquisito il consenso informato degli interessati ☐ sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati e il programma di ricerca comporta l'utilizzo di campioni biologici e di dati genetici che in origine non consentono di identificare gli interessati, ovvero che, a seguito di trattamento, non consentono di identificare i medesimi interessati e non risulta che questi ultimi abbiano in precedenza fornito indicazioni contrarie
Esercizio da parte dell'interessato dei diritti ex artt.15-22 DPR	
E' stata predisposta una procedura ad hoc da parte dell'Ente?	X Sì ☐ No

[1] il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

[2] Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità' all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento.

[3] Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

OECI COMPREHENSIVE Cancer Centre

A CURA DELL'AZIENDA U.S.L – IRCCS DI REGGIO EMILIA

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO		
MISURA	Esistenti	Note
Organigramma interno	X	
Nomine responsabili esterni	X	
Nomina DPO	X	
Informativa	X	
Istruzioni persone autorizzate trattamento	X	
Formazione	X	
Registri	X	
Procedure	X	
Politiche di tutela della privacy	X	
Distruzione/smaltimento sicuro cartaceo	X	
Inventario degli asset	X	
Misure anti – intrusive (cartelli di divieto di accesso ai locali, strumenti per la rilevazione degli accessi, guardiania, portineria, serrature armadi, schedari, ecc.)	X	
Politiche di sicurezza informatica	X	
Controllo accessi (log)	X	
Antivirus / firewall	X	
Politiche di clear screen	X	
Back – up dei dati	X	
Politiche di trasmissione dei dati	Allegare alla DPIA il Modulo relativo all'Archiviazione e Rilevazione Dati Per Attività di Ricerca su Sistemi Informativi	
nel caso si utilizzi un sito web esterno:		
Connessione sicura		
Accesso protetto da utenza personale		
Crittografia		
Anonimizzazione		
Pseudonimizzazione		
Sicurezza dei documenti cartacei	X	
Gestione postazioni	X	
Autenticazione	X	
Policy di gestione data breach	X	
Altro:		

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

OECI COMPREHENSIVE Cancer Centre

APPENDICE

MINACCE
ACCESSO ILLEGITTIMO AI DATI
Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare? Perdita di riservatezza dei dati personali coperti da segreto professionale; perdita del controllo dei propri dati; decifratura non autorizzata dei dati pseudonimizzati; diffusione dei dati non autorizzata **Quali sono le principali minacce che potrebbero concretizzare il rischio?** Utilizzo inappropriato delle password di accesso ai pc aziendali e al database di raccolta dati; sottrazione delle password di accesso da parte di un terzo; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; virus; accesso non autorizzato all'archivio delle cartelle cliniche dei pazienti arruolati nello studio **Quali sono le fonti di rischio?** Fonti umane interne (lasciare incustodita la postazione di lavoro, errore di integrazione applicativa). Fonti umane esterne (hacker). Fonti non umane (virus, applicativi che interoperano con il SW, introduzione di bug in seguito ad aggiornamento dell'applicativo) **Quali misure fra quelle individuate contribuiscono a mitigare il rischio?** Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); Antivirus/firewall; Politiche di trasmissione dei dati; Crittografia; Pseudonimizzazione **Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?** Bassa: l'impatto sugli interessati potrebbe essere elevato, tuttavia le misure previste per evitare gli accessi non autorizzati rendono limitata la probabilità di accadimento **Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?** Molto bassa: le politiche di sicurezza informatica e le misure adottate a protezione delle postazioni di lavoro e degli archivi cartacei rendono quasi nulla la probabilità di accadimento
MODIFICHE INDESIDERATE DEI DATI
Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare? Perdita di integrità del dato; la modifica potrebbe essere definitiva e avere conseguenze sulla attendibilità dei risultati dello studio fino a conseguenze sulla cura dei pazienti **Quali sono le principali minacce che potrebbero concretizzare il rischio?**

Utilizzo inappropriato delle password di accesso ai pc aziendali e al database di raccolta dati; sottrazione delle password di accesso da parte di un terzo; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; virus; accesso non autorizzato all'archivio delle cartelle cliniche dei pazienti arruolati nello studio

Quali sono le fonti di rischio?

Fonti umane interne (lasciare incustodita la postazione di lavoro, alterazione volontaria di dati, errore umano involontario). Fonti umane esterne (hacker). Fonti non umane (virus, applicativi che interoperano con il SW)

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

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); antivirus/firewall; Back – up dei dati

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

Bassa: l'impatto sugli interessati potrebbe essere elevato, tuttavia le misure di gestione dell'accesso all'applicativo e le misure adottate a protezione delle postazioni di lavoro riducono notevolmente la probabilità di accadimento.

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

Molto bassa: le misure adottate a protezione delle postazioni di lavoro e degli archivi cartacei rendono quasi nulla la probabilità di accadimento, la conservazione dei documenti contenenti dati personali e/o sensibili avviene in archivi ad accesso selezionato e controllato;

PERDITA DI DATI

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

Una perdita dei dati potrebbe causare l'alterazione dei risultati dello Studio o la impossibilità di proseguire lo Studio; tuttavia non si tratta di dati originali

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

La minaccia principale è quella di una distruzione o cancellazione erronea o volontaria dei dati
Le principali minacce possono essere di natura informatica (infezione da ransomware che blocca il sistema di accesso ai propri data base, provocando anche solo in modo temporaneo una impossibilità ad accedere al server, guasto che determina il danneggiamento, l'interruzione o la non disponibilità del sistema, che andando a colpirne elementi chiave possa mettere a rischio la disponibilità dei dati) o derivare da una azione umana (utilizzo improprio della posta elettronica da parte di un operatore attraverso cui un virus potrebbe bloccare il sistema aziendale; Incidente tecnico al datacenter (incendio, inondazione, fulmini…)

Quali sono le fonti di rischio?

Fonti umane interne (operatori autorizzati che abusino del proprio ruolo o colposamente operino cancellazioni sui dati per inesperienza o imperizia; lasciare incustodita la postazione di lavoro; lasciare incustodite sulla scrivania le cartelle cliniche dei pazienti arruolati nello Studio; errore progettuale/realizzativo che opera una modifica impropria ai dati gestiti); Fonti umane esterne (hacker); Fonti di rischio non umane (virus informatico; calamità naturali; guasto all'impianto elettro-idraulico del datacenter)

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

OECI COMPREHENSIVE Cancer Centre

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

Back – up dei dati; Controllo accessi (log); Misure anti – intrusive; antivirus/firewall; Tracciabilità, Gestione postazioni; Politiche di tutela della privacy¸ Politiche di sicurezza informatica

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

Molto bassa: i dati non sono originali, quindi l'impatto sugli interessati non è elevato, inoltre le misure previste per evitare la perdita dei dati rendono limitata la probabilità che essa si verifichi

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

Molto bassa: le misure adottate a protezione delle postazioni di lavoro e degli archivi cartacei rendono quasi nulla la probabilità di accadimento

VALUTAZIONE DEL RISCHIO

PROBABILITA' (P)	***IMPATTO (I)***	***RISCHIO (R=P*I)***
Probabilità molto bassa: 1	Impatto molto basso: 1	
Probabilità bassa: 2	Impatto basso: 2	Rischio basso: R< 7
Probabilità media: 3	Impatto medio: 3	Rischio medio: 7<R<11
Probabilità alta: 4	Impatto alto: 4	Rischio alto: R>11
Probabilità molto alta: 5	Impatto molto alto: 5	

MATRICE DI VALUTAZIONE DEL RISCHIO

		IMPATTO§§				
PROBABILITA'	**MOLTO ALTO§**	5	10	15	20	25
	ALTO	4	8	12	16	20
	MEDIO	3	6	9	12	15
	BASSO	2	4	6	8	10
	MOLTO BASSO	1	2	3	4	5
		MOLTO BASSO	**BASSO**	**MEDIO**	**ALTO**	**MOLTO ALTO**

§ Frequenza con la quale si possono verificare criticità nel trattamento dei dati: **Rischio molto basso**: è probabile che non si verifichi mai; **Basso**: non è probabile che si verifichi, ma può accadere; **Medio**: si può verificare occasionalmente; **Alto**: è probabile che si verifichi, ma non in modo persistente/stabile; **Molto alto**: è quasi certo che si verifichi, possibilmente in modo frequente

§§ Impatto atteso: **Molto basso**: è improbabile che possa avere un qualsiasi impatto; **Basso**: può avere un impatto; **Medio**: è probabile che abbia un impatto; **Alto**: molto probabile che abbia un impatto significativo; **Molto alto**: correlato ad un impatto maggiore

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

OECI COMPREHENSIVE Cancer Centre

MINACCIA	VALORE DEL RISCHIO (P*I)	LIVELLO DI RISCHIO	VALUTAZIONE COMPLESSIVA (SOMMA COLONNA LIVELLO RISCHIO)
ACCESSO ILLEGITTIMO	2*1	2	5
MODIFICHE INDESIDERATE DEI DATI	2*1	2	
PERDITA DI DATI	1*1	1	

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