

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



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: "Misura degli outcomes in pazienti con recidiva platino-sensibile di carcinoma ovarico epiteliale candidati a chirurgia citoreduttiva secondaria e (o chemioterapia in uno scenario reale. Uno studio retrospettivo multicentrico: RECOVeR (REcurrence OVarian cancer real Life)"

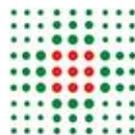
Codice di Protocollo: RECOVeR

Titolari del trattamento: Azienda U.S.L. – IRCCS di Reggio Emilia e Fondazione Policlinico Universitario A. Gemelli IRCCS, Roma

Principal Investigator: dr. Vincenzo Dario Mandato

S.C./S.S.D./Unità: Ostetricia e Ginecologia

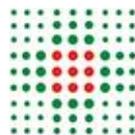
Data compilazione 11/11/2024



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



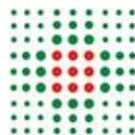
TRATTAMENTO DEI DATI	
Descrizione del trattamento (compilare i campi successivi o allegare il modulo di fattibilità dello studio)	
<p>Sinossi dello Studio</p>	<p>L'attuale standard di cura per la recidiva di carcinoma ovarico platino-sensibile (ROC) consiste in una combinazione di chirurgia citoriduttiva secondaria (SCS) e chemioterapia platinum-based secondo le principali linee guida internazionali.</p> <p>I dati retrospettivi e di meta-analisi hanno mostrato come la resezione macroscopica completa (CGR) del tumore seguita dalla chemioterapia adiuvante offra un vantaggio prognostico rispetto alla sola chemioterapia.</p> <p>Nel contesto degli studi randomizzati controllati (RCT), nello studio Desktop III, applicando una rigorosa selezione dei pazienti tramite l'AGO score, si è riscontrato un significativo vantaggio in termini di sopravvivenza, sia in termini di sopravvivenza globale (OS) che di sopravvivenza libera da progressione (PFS), nel braccio della chirurgia citoriduttiva rispetto al braccio della sola chemioterapia. In particolare, la CGR si è affermata come il principale fattore prognostico positivo con una OS mediana di 61,9 mesi in questo specifico sottogruppo di pazienti. In linea con questi risultati, lo studio SOC-1, selezionando i pazienti mediante una combinazione di i-MODEL e PET-TC, ha riscontrato una PFS significativamente più lunga nel gruppo SCS, mentre i risultati di OS debbono ancora essere maturati.</p> <p>Al contrario, il GOG 213 non è riuscito a dimostrare un vantaggio significativo della chirurgia rispetto alla chemioterapia platinum-based sia in PFS che in OS. In un'analisi di sottogruppo, tuttavia, la CGR sembrava avere un impatto positivo sulla PFS.</p> <p>Questi tre RCT, pur chiarendo meglio il ruolo del SCS, hanno lasciato alcune questioni aperte ed irrisolte.</p> <p>Lo stato della mutazione BRCA e la caratterizzazione molecolare del tumore stanno contribuendo a ridisegnare la definizione di sensibilità al platino; in tale contesto indagare la correlazione tra SCS e il profilo genetico del tumore risulta ad oggi prioritario.</p> <p>Infatti, nel contesto dei RCT, l'analisi BRCA non è stata riportata né sul GOG 213 e nemmeno sul Desktop III, mentre solo 75 pazienti sui 357 arruolati sono stati profilati per la mutazione germinale BRCA nello studio SOC-1 [5,6,7]. Inoltre, negli ultimi anni la terapia di mantenimento con agenti anti-angiogenetici (Bevacizumab) ed inibitori della poliADP-ribosio polimerasi (PARPi) è emersa in modo preponderante come standard di cura.</p> <p>Tuttavia, solo il 4,9% dei pazienti in Desktop III e circa il 10% in SOC-1 hanno beneficiato della terapia con PARPi, mentre l'84% dei pazienti in GOG 213, il 23% in DESKTOP III e l'1% nel SOC-1 hanno ricevuto il</p>



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



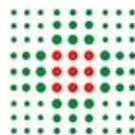
	<p>mantenimento con bevacizumab .</p> <p>Obiettivo primario: Valutare l'esito della chirurgia citoreduttiva secondaria (SCS) e/o della sola chemioterapia associata o meno a terapia di mantenimento con PARPi o Bevacizumab in uno scenario reale di pazienti affette da recidiva platino-sensibile di carcinoma ovarico il cui stato mutazionale BRCA/HRD sia disponibile.</p> <p>Obiettivi secondari:</p> <ul style="list-style-type: none"> • Descrivere le caratteristiche cliniche e molecolari dei pazienti sottoposti a citoreduzione secondaria e/o sola chemioterapia. • Descrivere le caratteristiche della citoreduzione secondaria e il suo esito in termini di resezione macroscopica completa (CGR). • Descrivere le complicanze intra e postoperatorie che si verificano entro 30 giorni dalla citoreduzione secondaria e il tempo necessario per intraprendere la chemioterapia. <p>Endpoint primari: Valutare gli outcomes oncologici misurati dalla sopravvivenza libera da progressione (PFS) e dalla sopravvivenza post-recidiva (PRS) in una serie di pazienti affette da recidiva platino-sensibile di carcinoma ovarico sottoposte a citoreduzione secondaria e/o chemioterapia e stratificati per mutazione BRCA/HRD e per terapia di mantenimento con PARPi o Bevacizumab.</p> <p>Endpoint secondari:</p> <ul style="list-style-type: none"> • Tutte le variabili considerate saranno riassunte per illustrarne le caratteristiche cliniche e genetiche e tabulate in base al trattamento ricevuto (SCS o solo chemioterapia). • La frequenza relativa di CGR sarà calcolata come rapporto tra il numero di CGR ottenute e il numero totale di pazienti sottoposte a SCS e tabulata in base alle caratteristiche dei pazienti. • Le complicanze intra e post-operatorie saranno classificate secondo le classificazioni Clavien-Dindo e CTCAE. <p>Popolazione target: Pazienti affette da recidiva platino-sensibile di carcinoma ovarico trattate con chirurgia citoreduttiva secondaria (SCS) e/o chemioterapia associata o meno a terapia di mantenimento con PARPi o Bevacizumab da Gennaio 2015 a Dicembre 2023.</p> <p>Criteri d'inclusione: Pazienti di età superiore ai 18 anni</p> <ul style="list-style-type: none"> • Diagnosi iniziale di carcinoma ovarico, delle tube di Falloppio o peritoneale di grado moderato/alto
--	--



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



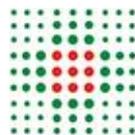
	<ul style="list-style-type: none"> • Diagnosi di prima recidiva platino-sensibile di carcinoma ovarico, delle tube di Falloppio o del peritoneo di grado moderato/alto • Pazienti sottoposti a chirurgia citoriduttiva secondaria o sola chemioterapia • Test BRCA e/o HRD disponibili • Firma del consenso informato oppure dichiarazione sostitutiva al modulo di consenso laddove applicabile <p>Criteri di esclusione:</p> <ul style="list-style-type: none"> • Pazienti giudicati unfit per la citoriduzione secondaria e/o la chemioterapia • Tumori ovarici borderline e carcinoma ovarico non epiteliale • Tumori di basso grado e mucinosi • Recidiva del tumore platinorefrattaria o platinoresistente (recidiva del tumore entro 3 o 6 mesi dal termine della chemioterapia a base di platino) • Test BRCA e/o HRD non disponibili <p>Durata dello studio: 24 mesi</p> <p>ANALISI STATISTICA e dimensionamento campionario se applicabile: Data la natura retrospettiva dello studio e l'obiettivo primario puramente descrittivo, non vengono prese in considerazione ipotesi formali e si stima di raggiungere un campione di circa 400 pazienti.</p> <p>DISEGNO DELLO STUDIO: Studio osservazionale retrospettivo, con farmaco multicentrico</p>
<p>Tipologia di dati raccolti</p>	
<p>Modalità di raccolta (fonte dei dati) (barrare anche più caselle)</p>	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> da cartelle cliniche/documentazione sanitaria <input checked="" type="checkbox"/> da archivi di dati clinici (esempio Dossier Sanitario - DWH) <input type="checkbox"/> da archivi di test diagnostici <input type="checkbox"/> da dati di laboratorio <input type="checkbox"/> da database amministrativi <input type="checkbox"/> altro (specificare) _____
<p>Trattamento dei dati (indicare il supporto utilizzato per la rilevazione e conservazione dei dati)</p>	<ul style="list-style-type: none"> <input type="checkbox"/> In formato cartaceo <input checked="" type="checkbox"/> In formato digitale <input type="checkbox"/> altro (specificare) _____



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



<p>Categorie di persone interessate</p>	<p><input checked="" type="checkbox"/> pazienti <input type="checkbox"/> persone sane <input type="checkbox"/> operatori sanitari <input type="checkbox"/> altro (specificare) _____</p>
<p>Categorie di dati trattati</p>	<p><input checked="" type="checkbox"/> dati sulla salute fisica o psichica <input type="checkbox"/> dati genetici <input type="checkbox"/> informazioni sulla vita sessuale <input type="checkbox"/> informazioni sull'orientamento sessuale <input type="checkbox"/> informazioni sugli stili di vita e/o le condizioni socioeconomiche <input type="checkbox"/> informazioni su istruzione e formazione professionale <input type="checkbox"/> anamnesi lavorativa <input type="checkbox"/> informazioni su religione o altre credenze <input type="checkbox"/> altro (specificare) _____</p>
<p>I dati personali (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati/condivisi con altri?</p>	<p><input type="checkbox"/> No <input checked="" type="checkbox"/> Sì Se sì, selezionare uno o più ambiti di comunicazione: <input checked="" type="checkbox"/> Promotore <input type="checkbox"/> CRO</p>
<p>I dati personali (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono trasferiti all'estero?</p>	<p><input checked="" type="checkbox"/> No <input type="checkbox"/> Sì Se sì <input type="checkbox"/> Paesi area UE <input type="checkbox"/> Paesi extra UE In quale/i Paese/i all'interno dell'area o extra UE _____</p>
<p>Misure di protezione dei dati</p>	

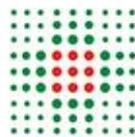


**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



Verranno conservati i dati identificativi dei partecipanti?	<input checked="" type="checkbox"/> No <input type="checkbox"/> Sì Se sì, specificare le ragioni sottese a tale esigenza: _____ _____ _____
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: <input type="checkbox"/> Adozione di tecniche crittografiche <input checked="" type="checkbox"/> 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 <input type="checkbox"/> Altro, specificare in dettaglio _____ _____ Per anonimizzare o aggregare i dati, anche in un momento successivo alla raccolta, sono adottate le seguenti misure: <input type="checkbox"/> I dati personali, a seguito della raccolta sono eliminati definitivamente senza la possibilità di risalire ai dati originali <input type="checkbox"/> I dati personali sono sostituiti 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 <input type="checkbox"/> Sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati <input type="checkbox"/> Altro (specificare) _____ _____

PRINCIPI, FINALITA' E BASI GIURIDICHE	
Necessità e proporzionalità	
Sono trattati solo i dati necessari e pertinenti al perseguimento delle finalità della ricerca (Minimizzazione)?	<input checked="" type="checkbox"/> Sì <input type="checkbox"/> No Se no, specificare i motivi e le azioni previste _____ _____ _____ _____
Integrità ed esattezza	



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



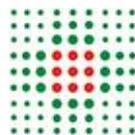
Sono state messe in campo azioni per garantire l'integrità ed esattezza dei dati?	<input checked="" type="checkbox"/> Sì <input type="checkbox"/> No Se no, specificare i motivi e le azioni previste _____ _____
Limitazione della conservazione	
Per quanto tempo verranno conservati i dati raccolti?	Indicare il numero di anni : 7 Decorso tale termine i dati verranno: <input type="checkbox"/> Anonimizzati completamente <input checked="" type="checkbox"/> distrutti <input type="checkbox"/> altro (<i>specificare</i>) _____
Basi giuridiche	
Quali sono le basi giuridiche del trattamento?	<input type="checkbox"/> art. 9, par. 2, lett. j) GDPR ¹ <input type="checkbox"/> art. 110, co. 1 primo periodo Codice Privacy ² <input checked="" type="checkbox"/> 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)	<input type="checkbox"/> motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione <input checked="" type="checkbox"/> sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati in ragione: <input type="checkbox"/> del numero molto alto di interessati che è stato stimato

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.

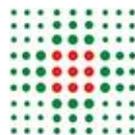
³ Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.



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



<i>interessati) e acquisirne il consenso</i>	<input checked="" type="checkbox"/> deceduti o non contattabili
<i>Nel caso di studi retrospettivi su dati genetici, ove non sia possibile ottenere il consenso informato, indicare se ricorrono le condizioni indicate</i>	<input type="checkbox"/> indagini statistiche o ricerche scientifiche previste dal diritto dell'Unione europea, dalla legge o, nei casi previsti dalla legge, da regolamento <input type="checkbox"/> scopi scientifici e statistici direttamente collegati con quelli per i quali è stato originariamente acquisito il consenso informato degli interessati <input type="checkbox"/> 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	
<i>E' stata predisposta una procedura ad hoc da parte dell'Ente?</i>	<input checked="" type="checkbox"/> Sì <input type="checkbox"/> No

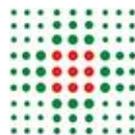


**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



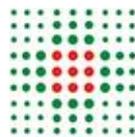
A CURA DELL'AZIENDA U.S.L – IRCCS DI REGGIO EMILIA

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 nel caso si utilizzi un sito web esterno:		Allegare alla DPIA il Modulo relativo all'Archiviazione e Rilevazione Dati Per Attività di Ricerca su Sistemi Informativi
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:		



APPENDICE

MINACCE
ACCESSO ILLEGITTIMO AI DATI
<p>Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?</p> <p>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</p> <p>Quali sono le principali minacce che potrebbero concretizzare il rischio?</p> <p>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; accesso non autorizzato all'archivio delle cartelle cliniche dei pazienti arruolati nello studio; virus</p> <p>Quali sono le fonti di rischio?</p> <p>Fonti umane interne (lasciare incustodita la postazione di lavoro, lasciare incustodite sulla scrivania le cartelle cliniche dei pazienti arruolati nello studio, 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)</p> <p>Quali misure fra quelle individuate contribuiscono a mitigare il rischio?</p> <p>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; Anonimizzazione; Pseudonimizzazione</p> <p>Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?</p> <p>Media</p> <p>Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?</p> <p>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</p>
MODIFICHE INDESIDERATE DEI DATI
<p>Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?</p> <p>Perdita di integrità del dato; la modifica potrebbe essere definitiva e avere conseguenze sulla cura del paziente</p> <p>Quali sono le principali minacce che potrebbero concretizzare il rischio?</p> <p>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; accesso non autorizzato all'archivio delle cartelle cliniche dei pazienti arruolati nello studio; virus</p> <p>Quali sono le fonti di rischio?</p> <p>Fonti umane interne (lasciare incustodita la postazione di lavoro, lasciare incustodite sulla scrivania le cartelle cliniche dei</p>



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



pazienti arruolati nello studio, 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

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

Media: nonostante le misure adottate a protezione delle postazioni di lavoro, lo strumento utilizzato per la allocazione dei dati (excel) non è da ritenere del tutto sicuro rispetto alla probabilità di accadimento

PERDITA DI DATI

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

Una perdita dei dati potrebbe essere sia informatica che cartacea; in entrambi i casi potrebbe causare l’alterazione dei risultati dello Studio o la impossibilità di proseguire lo Studio

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; accesso non autorizzato ai locali archivio causando la sottrazione del materiale cartaceo, se il formato cartaceo è l’unico sistema di conservazione del dato e non esiste alcun backup). 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)

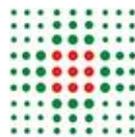
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

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: l’impatto sugli interessati potrebbe essere elevato, tuttavia le misure previste per evitare la perdita dei dati rende 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?



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



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

A CURA DEL DPO

VALUTAZIONE DEL RISCHIO

<i>PROBABILITA' (P)</i>	<i>IMPATTO (I)</i>	<i>RISCHIO (R=P*I)</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	
Probabilità molto alta: 5	Impatto molto alto: 5	Rischio alto: $R > 11$

MATRICE DI VALUTAZIONE DEL RISCHIO

		IMPATTO ^{§§}				
		MOLTO ALTO [§]	ALTO	MEDIO	BASSO	MOLTO BASSO
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

<u>MINACCIA</u>	<u>VALORE DEL RISCHIO (P*I)</u>	<u>LIVELLO DI RISCHIO</u>	<u>VALUTAZIONE (SOMMA COLONNA LIVELLO RISCHIO)</u>
ACCESSO ILLEGITTIMO	3*1	3	10
MODIFICHE INDESIDERATE DEI DATI	2*3	6	
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