



VALUTAZIONE D'IMPATTO PER PROGETTI DI RICERCA IN AMBITO SANITARIO SU DATI RETROSPETTIVI

(ART. 110 D. LGS. 196/2003 s.m.i., Provvedimento Garante n. 146/2019)

La valutazione di impatto (DPIA- data protection impact assessment) 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.

Titolo dello studio

Programma di ricerca sanitaria finalizzata dell'Emilia-Romagna (FIN-RER): Risultati sul medio e lungo termine nei pazienti eradicati del virus dell'HCV in rapporto allo stadio di malattia al momento del trattamento

Codice di Protocollo

N/A

Titolare del trattamento: AZIENDA OSPEDALIERO-UNIVERSITARIA DI MODENA

Struttura/Dipartimento/U.O./Servizio UO Gastroenterologia

Soggetto delegato: Prof.ssa Erica Villa

Data compilazione 08 Aprile 2022

TRATTAMENTO DEI DATI	
Descrizione del trattamento <i>(compilare i campi successivi)</i>	
Obiettivi dello studio	Valutare, sul medio e lungo termine, la percentuale di pazienti che dopo terapia con farmaci antivirali diretti (DAA) per il trattamento dell'HCV, in rapporto allo stato di malattia all'inizio del trattamento, hanno a) sviluppato SVR b) in caso di fallimento terapeutico al primo trattamento, hanno risposto al ritrattamento c) avuto un miglioramento o un peggioramento

Versione 28 luglio 2021

	della condizione di malattia di base, valutata sia dal punto di vista funzionale, che della stiffness epatica d) avuto una regressione di uno stato di scompenso (soprattutto in termini di scompenso ascitico): i dati relativi a questo obiettivo sono molto scarsi in letteratura, perché i pazienti con malattia avanzata sono stati inclusi solo in pochissimi studi e) contratto nuovamente l'infezione HCV ed in che percentuale rispetto alla popolazione trattata Primario: Valutare la percentuale di soggetti che hanno sviluppato un carcinoma epatico primitivo (HCC) o una recidiva dello stesso, dopo trattamento con i DAA. Se gli antivirali diretti facilitino o meno l'insorgenza di HCC è uno dei punti ancora maggiormente sub judice. Poiché dati pubblicati di uno dei centri prescrittori della RER suggeriscono che i DAA agiscano come scatenanti l'HCC solo nei soggetti con severa ipertensione portale, la possibilità di fare una verifica su grandi numeri in soggetti con tutte le gradazioni di ipertensione portale potrà permettere di valutare l'effettivo rischio pro-carcinogeno. Come riferimento di confronto per valutare l'incidenza dei vari eventi, utilizzeremo i dati dello studio Uni-Rer_2 (vedi addendum a Metodologia e analisi statistica). L'incidenza di HCC nella coorte Uni-Rer_2_HCV è stata del 1.85 % dei cirrotici arruolati nel intervallo nei primi 3 anni dall'arruolamento (in cui i pazienti non sono stati trattati con i DAAs). Questo significherebbe un numero atteso di circa 100 casi di HCC nei 5000 cirrotici nella coorte del presente studio se i DAAs non avessero azione negativa ma un numero molto maggiore, raddoppiato, se i DAAs giocassero un ruolo sfavorevole. Valutare se, a parità di percentuale di risposta virale sostenuta nei due sessi, ci sia un simile impatto sulla prognosi. Non è noto se i DAA agiscano diversamente sul rischio tumorale nei due sessi. Particolarmente rilevante sarebbe la valutazione del rischio di sviluppo di HCC nei due sessi: nella fascia di età di picco dei trattamenti (50-70 anni) il rischio tumorale, che per la donna in età pre-menopausale è molto più basso che nell'uomo, i diventa non significativamente differente da quello dell'uomo. I dati dello studio Uni-Rer_2 confermano che la correttezza dell'assunto, indicando un'incidenza di HCC del 2.2% e del 3.2% nei maschi e dello 0.44% e dell'1.7% nelle donne prima e dopo l'età assimilabile alla menopausa.
Breve sintesi del progetto	Background: L'infezione da virus dell'epatite C (HCV) è stata per molti anni la principale causa di malattia epatica cronica e di tumore epatocellulare (HCC) e di conseguenza, anche di trapianto di fegato. Per molto tempo la terapia si è basata pressoché esclusivamente sugli interferoni, prima normali, poi peghilati (usati da soli o in associazione con gli inibitori delle proteasi di prima generazione), che, oltre ad avere scarsa tollerabilità, non ottenevano più del 30-35% di risposta a lungo termine (SVR). L'avvento dei nuovi farmaci antivirali diretti (DAA) ormai quasi 10 anni fa ha completamente cambiato lo scenario, sia dal punto di vista della straordinaria tollerabilità e mancanza di effetti collaterali (che ne hanno reso possibile l'uso anche in pazienti con condizioni cliniche non ottimali) che da quello dei risultati. Anche con i primi farmaci resisi disponibili, sicuramente non così potenti come quelli attualmente in uso, le risposte a lungo termine superavano il 70%. Attualmente, grazie ai DAAs di ultima generazione, la SVR anche nei casi caratterizzati dai genotipi come il 3 più difficili da trattare o in presenza di malattia cirrotica avanzata (condizione clinica che rende più difficile ottenere l'eliminazione virale) o di co-morbidità importanti sfiora il 100% Dall'inizio della disponibilità dei DAA (dicembre 2014), in Emilia-Romagna sono stati trattati oltre 18.000 soggetti HCV-positivi, inizialmente con malattia molto avanzata, poi progressivamente meno severa, in periodi temporali chiaramente identificabili, perché corrispondenti ai successivi allargamenti dei criteri di trattamento dettati da AIFA. Questo offre una possibilità unica di valutare se esista un differente guadagno prognostico a seconda dello stadio di malattia e se questi gruppi omogenei di pazienti abbiano un rischio diverso di sviluppare HCC, potenzialmente in relazione con lo stadio di malattia ed il livello di ipertensione portale Durata dello Studio Durata Prevista: 36 Mesi dall'ottenimento dell'autorizzazione aziendale Data di fine prevista Aprile 2025 Disegno dello Studio/metodologia I dati di esito saranno raccolti in tutte le UO che costituiscono la rete HCV regionale e che coprono l'intero territorio regionale ma il coordinamento dei 3 WPs sarà affidato a gruppi di 3 UO, per competenza specifica. WP1: punto critico per la buona riuscita del progetto è che la raccolta dati sia capillare, esaustiva e che sia in grado di raccogliere con precisione i dati di esito della terapia di ogni caso che è già stato arruolato. Questo implica un convinto coinvolgimento di tutte le Unità Operative che hanno trattato i pazienti con infezione da HCV. Per la raccolta dati

Versione 28 luglio 2021

	verrà implementata una eCRF standardizzata accessibile da ogni singolo centro attraverso il proprio server aziendale. La eCRF (REDCap) sarà in grado di gestire un rilevante numero di casi inseriti (che oscilleranno da centro a centro dai 2500 ai 3500 circa). Ogni centro condurrà l'analisi statistica sui propri pazienti secondo le indicazioni date dal centro coordinatore ai centri deputati alle analisi di sottogruppo, a cui perverranno però solo i dati aggregati dell'analisi condotta da ogni centro. L'analisi statistica finale verrà quindi condotta sui soli dati aggregati provenienti da ogni centro. • WP2: questo WP elaborerà in modo specifico i dati aggregati relativi al rischio di sviluppo di HCC de novo o di recidiva dopo terapia con DAA. Il tema è ancora molto dibattuto in quanto solo pochi studi hanno avuto la possibilità di esaminare un numero elevato di Pazienti, trattati con protocolli di accesso uniformi come è stato fatto nella RER (UO 4-6). • WP3: Questo WP sarà dedicato a valutare l'esito della terapia nei soggetti co-infetti HCV-HIV e HCV/HBV, sfruttando la presenza nella rete esistente di numerose UO di Malattie Infettive. Acquisire il dato di esito nei Pazienti co-infetti con HIV o con HBV è grandemente rilevante in quanto la malattia HCV/HIV decorre in modo più veloce e ha una prognosi più severa della monoinfezione HCV mentre la co-infezione con HBV potrebbe aumentare il rischio tumorale (UO 7-9). Anche questi dati verranno analizzati come dati aggregati. Materiali e metodi dello Studio Nel periodo 2015-luglio 2020 sono stati trattati con DAA nella RER 17.857 soggetti HCV+. Lo studio prevede la raccolta e l'elaborazione, per tutti i pazienti sottoposti a trattamento con i DAA, dei dati clinici, demografici e di outcome (in termini di 1. risposta a lungo termine, 2. non risposta è necessità di ritrattamento, 3. sviluppo di scompenso, 4. sviluppo di tumore epatico primitivo (HCC) e 5. mortalità). La necessità di avere dati completi e esaustivi per tutti gli outcome di interesse rende obbligatorio il recupero dei dati dei pazienti mediante un lavoro di recupero dalle cartelle individuali, effettuato da ciascuna Unità operativa coinvolta in autonomia. I dati saranno trasferiti al centro coordinatore AOU di Modena solo in forma aggregata. I dati presenti nelle schede autorizzative al trattamento (schede compilate sulla apposita sezione "trattamenti" all'interno del ProgettoSole – Piattaforma istituita dalla Regione Emilia Romagna per il monitoraggio dei soggetti trattati con DAAs) non contengono infatti dati sufficienti per valutare gli outcome di interesse. Questo implica: 1) l'acquisizione diretta delle informazioni dalle cartelle cliniche. Nel caso che non sia possibile raccogliere il Consenso informato scritto dei soggetti arruolati per motivi etici e/o organizzativi in linea con quanto previsto dalla ratio delle disposizioni di cui al GDPR 2016/679 e dell'Autorizzazione Generale n. 9/2016, come modificata e integrata con Provvedimento n. 146/2019, verranno comunque acquisite le informazioni fermo restando che verrà fatto ogni sforzo per acquisire il consenso dei Pazienti che risultino reperibili e/o qualora sia possibile rendere loro un'adeguata informativa in particolare laddove questi si rivolgano al centro di cura, anche per visite di controllo. 2) l'impiego di data manager dedicati, afferenti alle Unità Operative delle singole Aziende Ospedaliere e/o Territoriali, in modo che la numerosità del campione non ostacoli l'acquisizione accurata dei dati di interesse. La natura osservazionale dello studio preclude la possibilità di un gruppo di controllo (peraltro eticamente difficilmente accettabile per le caratteristiche di elevata efficacia della terapia con DAAs in termini di risposta virologica sostenuta in tutte le categorie di pazienti HCV-positivi arruolati negli studi registrativi). Come parametri di confronto utilizzeremo i dati di uno studio prospettico iniziato nel 2012 che si propone di studiare i fattori biologici e clinici che predispongono allo sviluppo di HCC nei pazienti con fibrosi epatica avanzata e cirrosi epatica compensata (Uni-Rer_2) (quindi una categoria di pazienti assimilabile a quella trattata con i DAAs, che per indicazioni AIFA dovevano essere Child-Pugh A o B). Lo studio ha arruolato 606 pazienti (70% di sesso maschile) con malattia epatica cronica di diversa eziologia, di cui il 40% HCV-positivi. Lo studio Uni-Rer_2 ci permette di calcolare sia l'incidenza degli episodi di scompenso epatico (in quanto questa informazione è stata raccolta come possibile fattore eziologico collegato allo sviluppo di HCC), che quella di HCC e la mortalità, oltre che permettere le stesse analisi per sottogruppi (sesso; comorbidità quali diabete obesità etc.). Come esempio, l'incidenza di HCC nei pazienti cirrotici HCV-positivi nei primi tre anni dall'inizio dello studio è stata dell'1.8% mentre nei 4 anni successivi (dopo l'introduzione dei DAAs) è stata del 4.0%. I dati dello studio Uni-Rer_2 indicano anche che è lecito aspettarsi un notevole numero di eventi, anche nei primi anni dell'osservazione retrospettiva. Dati del nostro gruppo e di altri
--	---

Versione 28 luglio 2021

	(10.1053/j.gastro.2018.04.008) indicano che il tempo di comparsa dell'HCC dopo esposizione ai DAAs oscilla fra i 2 ed i 24 mesi: il lasso di tempo di osservazione che ci proponiamo di coprire è di 9 anni retrospettivo quindi sufficientemente ampio per identificare la maggioranza degli eventi, anche nei soggetti con malattia senza cirrosi clinica (cioè fibrosi F3). In questo sottogruppo, i dati dello studio Uni-Rer_2 indicano un'incidenza del 2.0% anche nei soggetti con HVPg<7, assimilabili quindi a soggetti con fibrosi F3. Considerazioni etiche Lo Studio prevede di raccogliere il Consenso informato scritto dei soggetti arruolati Lo studio non garantisce che sia sempre possibile raccogliere il consenso informato dei pazienti potenzialmente arruolabili, in quanto alcuni di essi potrebbero risultare deceduti o non contattabili, ai sensi del Provvedimento del Garante Privacy n. 146/2019. I dati dei pazienti deceduti o non contattabili verranno trattati in conformità alle previsioni di cui all'art. 110 del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018. Nel caso che non sia possibile raccogliere il Consenso informato scritto dei soggetti arruolati per motivi etici e/o organizzativi in linea con quanto previsto dalla ratio delle disposizioni di cui al GDPR 2016/679 e del suddetto Provvedimento n. 146/2019, verranno comunque acquisite le informazioni fermo restando che verrà fatto ogni sforzo per acquisire il consenso dei Pazienti che risultino reperibili e/o qualora sia possibile rendere loro un'adeguata informativa in particolare laddove questi si rivolgano al centro di cura, anche per visite di controllo. Non sarà necessario informare la figura del MMG dei soggetti coinvolti nello studio. La natura osservazionale e la tipologia retrospettiva delle indagini e delle analisi, nonché l'assenza di somministrazione di una terapia, rende superfluo il coinvolgimento del MMG Ricaduta dello Studio I vantaggi per il SSR si posizionano a diversi livelli: - clinico: i due end-points che ci prefiggiamo di valutare (sopravvivenza e sviluppo di tumore del fegato) sono fra i più rilevanti per un paziente. Identificare i candidati che più verosimilmente avranno un esito migliore in termini di sopravvivenza o che di converso non abbiano impatti negativi dalla terapia con DAA come lo sviluppo di un HCC è di estrema importanza; - economico: il punto precedente ha una ricaduta immediata anche per quanto riguarda l'impatto economico, non solo diretto, come costo dei DAA, ma anche indiretto, come risparmio di risorse sanitarie per evitato sviluppo, ad esempio, di una patologia cirrotica o tumorale. L'esatta valutazione degli esiti clinici porta ad una più precisa possibilità di pianificazione economica; - organizzativo: ogni progressione di malattia evitata comporta non solo un risparmio economico ma anche organizzativo, soprattutto in termini di giornate di degenza evitate per evitata progressione di malattia.
Promotore	Azienda Ospedaliero-Universitaria di Modena
Tipologia di dati raccolti	
Modalità di raccolta (barrare anche più caselle)	☒ consultazione cartelle cliniche/documentazione sanitaria ☐ archivi di dati clinici ☐ archivi di test diagnostici ☐ dati di laboratorio ☐ altro (specificare)
Trattamento dei dati (indicare il supporto utilizzato per la rilevazione e conservazione dei dati)	☐ In formato cartaceo ☒ In formato digitale ☐ altro (specificare)

Categorie di persone interessate	☒ Pazienti ☐ persone sane ☐ operatori sanitari ☐ soggetti vulnerabili ☐ altro (specificare)
Categorie di dati trattati	☒ dati sulla salute fisica o psichica ☐ dati genetici ☐ informazioni sulla vita sessuale ☐ informazioni sull'orientamento sessuale ☐ informazioni sugli stili di vita e 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 ☐ Sì Se sì, selezionare uno o più ambiti di comunicazione: ☐ Promotori ☐ CRO ☐ altro (specificare)
I dati personali (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono trasferiti all'estero?	☒ 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 soggetti dello studio?	☐ No ☒ Sì Se sì, specificare le ragioni sottese a tale esigenza: per eventuale monitoraggio della correttezza delle informazioni raccolte i dati saranno conservati esclusivamente nella patient identification list.

<i>Descrivere le procedure utilizzate per</i> a) non identificare direttamente o pseudonimizzare b) rendere anonimi i dati dei partecipanti nelle diverse fasi della ricerca	a) Per non identificare direttamente l'interessato o pseudonimizzare sono adottate le seguenti misure: ☐ Adozione di tecniche crittografiche (dei dati identificativi del soggetto) ☒ 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 ☐ Altro, specificare in dettaglio _____ b) Per rendere anonimi 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 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 ☐ 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	
<i>Sono trattati solo i dati necessari e pertinenti al perseguimento delle finalità della ricerca (Minimizzazione)?</i>	☒ Sì ☐ No Se no, specificare i motivi e le azioni previste _____ _____ _____ _____
Integrità ed esattezza	
<i>Sono state messe in campo azioni per garantire l'integrità ed esattezza dei dati?</i>	☒ 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 mesi/anni <u>7 anni</u> Decorso tale termine i dati verranno: ☐ Anonimizzati completamente ☒ Distrutti ☐ altro (<i>specificare</i>) _____
Basi giuridiche	
Quali sono le basi giuridiche del trattamento?	☐ art. 9, par. 2, lett. j) GDPR¹ ☐ art. 110, co. 1 primo periodo Codice Privacy² ☒ art. 110, co. 1, secondo periodo Codice Privacy³ ☐ art. 110 bis, co. 4: Istituto di Ricerca e Cura a carattere scientifico per le attività di assistenza e ricerca dell'ambito di riconoscimento⁴

MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO	
Informativa e consenso	
SOLO SE LA BASE GIURIDICA È L'ART. 110, CO. 1, SECONDO PERIODO <i>Indicare i motivi per i quali non è possibile fornire l'informativa ai partecipanti allo Studio (soggetti interessati) e acquisirne il consenso</i>	☐ motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione ☒ sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati in ragione: ☒ del numero molto alto di interessati che è stato stimato* ☒ deceduti o non contattabili* * > 17000 interessati
<i>Nel caso di studi retrospettivi su dati genetici, ove non sia possibile ottenere il consenso informato, indicare se ricorrono le condizioni indicate</i>	☐ 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

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.

⁴ Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento.
[ndr: Eccezione prevista per gli IRCCS con riferimento al trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici, per il quale i titolari non IRCCS devono effettuare la DPIA e richiedere il parere del Garante]

	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 GDPR	
E' stata predisposta una procedura ad hoc da parte dell'Ente?	☒ Sì ☐ No

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO Azienda Ospedaliero-Universitaria di Modena		
MISURA	Esistenti	Note
Organigramma interno	X	Delibera 150 del 06/09/2018
Nomine responsabili esterni	Non sono presenti	
Nomina DPO	X	Delibera 90 del 16/05/2018
Informativa	X	Sempre presente
Istruzioni persone autorizzate trattamento	X	Le persone autorizzate al trattamento sono state correttamente istruite dal PI
Formazione	X	Self training del team dello Studio
Registri	Non sono presenti	Non sono presenti dei registri specifici
Procedure	Non sono presenti	Non sono presenti delle procedure specifiche
Politiche di tutela della privacy	X	AOUMO ha nominato un DPO e all'interno dell'Azienda esiste un Gruppo aziendale Privacy - al quale afferiscono, tra gli altri membri, il Direttore del Servizio Tecnologie dell'Informazione e il Referente aziendale Data Breach - che ha il compito di garantire e coordinare le attività aziendali correlate alla normativa in materia di protezione dei dati personali, supportando il Titolare del trattamento negli adempimenti previsti dalla normativa (Regolamento EU 2016/679, Decreto Legislativo 196/2003 e s.m.i.). Il Responsabile del Settore legale, assicurazioni e privacy si interfaccia con il Data Protection Officer e coordina il Gruppo aziendale Privacy. L'Azienda ha adottato un Regolamento in materia di Protezione Dati (Delibera 216 del 20/12/2019)
Distruzione/smaltimento sicuro cartaceo	X	Non pertinente
Inventario degli asset	X	Le postazioni di lavoro aziendali sono censite nel programma di gestione aziendale. Il SW utilizzato per la compilazione delle eCRF è RedCap® installato presso il datacenter aziendale
Misure anti – intrusive (cartelli di divieto di accesso ai locali, strumenti per la rilevazione degli accessi, guardiania, portineria, serrature armadi, schedari, ecc.)	X	I sistemi server sono ospitati presso il Data Center aziendale che risponde ai requisiti tier 3 ed anche i Datacenter regionali gestiti da Lepida S.c.p.A rispondono ai requisiti tier 3.
Politiche di sicurezza informatica	X	Sulle postazioni aziendali e sui web server viene garantito l'aggiornamento dei Sistemi Operativi e di un programma di antivirus e di

Versione 28 luglio 2021

		anti-malware completo. Sul server è anche attivo il firewall locale
Controllo accessi (log)	X	Essendo una cartella condivisa non sono presenti politiche di audit all'accesso
Antivirus / firewall	X	Presente sul firewall del file server
Politiche di clear screen	X	Non pertinente
Back – up dei dati	X	La cartella condivisa utilizzata come unità di memorizzazione dello studio è situata nei file server aziendali e viene quotidianamente salvata attraverso le normali procedure di Backup aziendali su due copie, una locale e una remota presso il datacenter di Lepida di Ferrara
Politiche di trasmissione dei dati	X	Per questo studio non vengono trasmessi i dati all'esterno dell'Azienda Ospedaliero Universitaria di Modena
nel caso si utilizzi un sito web accessibile dall'esterno:	x	Per questo studio si usa un sito WEB accessibile dall'esterno
Connessione sicura	x	Il sito web del questionario è raggiungibile esclusivamente tramite connessione protetta https
Accesso protetto da utenza personale		L'accesso al questionario è possibile solo tramite autenticazione integrata con Active directory aziendale
Crittografia	X	La banca dati su cui risiede il questionario è crittografata
Anonimizzazione	NA	NA
Pseudonimizzazione	X	I dati saranno Pseudoanonimizzati
Sicurezza dei documenti cartacei	X	I dati non vengono raccolti in formato cartaceo
Gestione postazioni	X	Le postazioni sono accessibili dai soli utenti aziendali. È presente un disciplinare aziendale sull'utilizzo delle postazioni informatiche
Autenticazione	X	L'autenticazione avviene tramite username/password. La password è cambiata ogni 90 giorni secondo le normative vigenti
Policy di gestione data breach	X	L'Azienda ha adottato una procedura di gestione delle violazioni dei dati personali in cui sono definite le modalità operative da seguire in caso di incidente. La medesima procedura viene fornita ai Responsabili del trattamento in quanto disciplina anche le violazioni esterne all'Azienda. È previsto un registro aziendale delle violazioni
Altro:		

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

Versione 28 luglio 2021

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

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; 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 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 causare l'alterazione dei risultati dello Studio.

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; accesso non autorizzato all'archivio delle cartelle cliniche dei pazienti arruolati nello studio; virus

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; 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?

Molto bassa: trattandosi di dati pseudonimizzati l'impatto sui pazienti di una modifica indesiderata è praticamente nullo

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 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; i locali in cui sono conservati tali documenti devono essere chiusi al termine dell'orario di lavoro

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 colpire 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; 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 Basso: non trattandosi di dati originali e per di più essendo i dati pseudoanonimizzati, la loro perdita ha un impatto sugli interessati praticamente nullo.

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

MINACCIA	VALORE DEL RISCHIO (P*I)	LIVELLO DI RISCHIO	VALUTAZIONE COMPLESSIVA (SOMMA COLONNA LIVELLO RISCHIO)
ACCESSO ILLEGITTIMO	2*1	2	4
MODIFICHE INDESIDERATE DEI DATI	1*1	1	

Versione 28 luglio 2021

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

