

**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** Presa in carico presso l'ambulatorio "MOvement and REhabilitation (MO.RE.)": uno studio osservazionale retrospettivo sull'appropriatezza di accesso e i bisogni espressi dai pazienti. (BACKMORE2024)

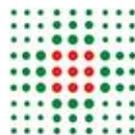
**Codice di Protocollo** BACKMORE2024

**Titolare/i del trattamento:** Azienda U.S.L. – IRCCS di Reggio Emilia

**Principal Investigator:** Stefania Fugazzaro

S.C./S.S.D./Unità S.C. di Medicina Fisica e Riabilitativa dell' AUSL-IRCCS di Reggio Emilia - Presidio Ospedaliero Provinciale Santa Maria Nuova

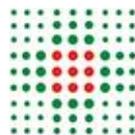
**Data compilazione** 01.10.2024



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



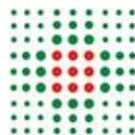
TRATTAMENTO DEI DATI	
Descrizione del trattamento (compilare i campi successivi o allegare il modulo di fattibilità dello studio)	
<b>Sinossi dello Studio</b>	<p>Per le informazioni di questo campo allego il modulo di fattibilità.</p> <p>Inoltre, si precisa che saranno previsti nel centro di Reggio Emilia un numero stimato di circa 100 pazienti (saranno inclusi tutti i pazienti che hanno avuto accesso all'ambulatorio MO.RE. nel periodo agosto 2022-giugno 2024)</p>
Tipologia di dati raccolti	
<b>Modalità di raccolta</b> (fonte dei dati) (barrare anche più caselle)	<input checked="" type="checkbox"/> X da cartelle cliniche/documentazione sanitaria <input checked="" type="checkbox"/> X 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) _____
<b>Trattamento dei dati</b> (indicare il supporto utilizzato per la rilevazione e conservazione dei dati)	<input type="checkbox"/> In formato cartaceo <input checked="" type="checkbox"/> X In formato digitale <input type="checkbox"/> altro (specificare) _____
<b>Categorie di persone interessate</b>	<input checked="" type="checkbox"/> X pazienti <input type="checkbox"/> persone sane <input type="checkbox"/> operatori sanitari <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><b>Categorie di dati trattati</b></p>	<p> <input checked="" type="checkbox"/> X 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 checked="" type="checkbox"/> X informazioni sugli stili di vita e/o le condizioni socioeconomiche  <input checked="" type="checkbox"/> X informazioni su istruzione e formazione professionale  <input checked="" type="checkbox"/> X anamnesi lavorativa  <input type="checkbox"/> informazioni su religione o altre credenze  <input type="checkbox"/> altro (specificare)  <hr/> </p>
<p><b>I dati personali (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati/condivisi con altri?</b></p>	<p> <input checked="" type="checkbox"/> X No  <input type="checkbox"/> Sì                  Se sì, selezionare uno o più ambiti di comunicazione:  <input type="checkbox"/> Promotore  <input type="checkbox"/> CRO             </p>
<p><b>I dati personali (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono trasferiti all'estero?</b></p>	<p> <input checked="" type="checkbox"/> X 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  <hr/> </p>
<p><b>Misure di protezione dei dati</b></p>	
<p><b>Verranno conservati i dati identificativi dei partecipanti?</b></p>	<p> <input type="checkbox"/> No  <input checked="" type="checkbox"/> X Sì                  Se sì, specificare le ragioni sottese a tale esigenza:  <hr/>                 i dati verranno conservati per consentire l'elaborazione e l'analisi descritte  <hr/> </p>

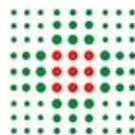


**SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA**  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



<p><b>Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca</b></p>	<p>Per non identificare direttamente l'interessato sono adottate le seguenti misure:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Adozione di tecniche crittografiche</li> <li><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</li> <li><input type="checkbox"/> Altro, specificare in dettaglio</li> </ul> <p>_____</p> <p>_____</p> <p>Per anonimizzare o aggregare i dati, anche in un momento successivo alla raccolta, sono adottate le seguenti misure:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> I dati personali, a seguito della raccolta sono eliminati definitivamente senza la possibilità di risalire ai dati originali</li> <li><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</li> <li><input type="checkbox"/> Sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati</li> <li><input type="checkbox"/> Altro (specificare)</li> </ul> <p>_____</p> <p>_____</p>
---	--

PRINCIPI, FINALITA' E BASI GIURIDICHE	
<b>Necessità e proporzionalità</b>	
<p><b>Sono trattati solo i dati necessari e pertinenti al perseguimento delle finalità della ricerca (Minimizzazione)?</b></p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Sì</li> <li><input type="checkbox"/> No</li> </ul> <p>Se no, specificare i motivi e le azioni previste _____</p> <p>_____</p> <p>_____</p>
<b>Integrità ed esattezza</b>	
<p><b>Sono state messe in campo azioni per garantire l'integrità ed esattezza dei dati?</b></p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Sì</li> <li><input type="checkbox"/> No</li> </ul> <p>Se no, specificare i motivi e le azioni previste _____</p> <p>_____</p>
<b>Limitazione della conservazione</b>	



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



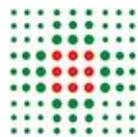
<b>Per quanto tempo verranno conservati i dati raccolti?</b>	Indicare il numero di mesi/anni 7 anni _____  Decorso tale termine i dati verranno: <input type="checkbox"/> Anonimizzati completamente x Distrutti <input type="checkbox"/> altro ( <i>specificare</i> ) _____
<b>Basi giuridiche</b>	
<b>Quali sono le basi giuridiche del trattamento?</b>	<input type="checkbox"/> art. 9, par. 2, lett. j) GDPR <sup>1</sup> <input type="checkbox"/> art. 110, co. 1 primo periodo Codice Privacy <sup>2</sup> <input checked="" type="checkbox"/> X art. 110, co. 1, secondo periodo Codice Privacy <sup>3</sup>

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

<sup>1</sup> 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.

<sup>2</sup> 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.

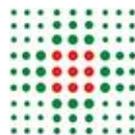
<sup>3</sup> Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.



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



	<p>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</p>
<b>Esercizio da parte dell'interessato dei diritti ex artt.15-22 DPR</b>	
<p><i>E' stata predisposta una procedura ad hoc da parte dell'Ente?</i></p>	<p>X Sì <input type="checkbox"/> No</p>

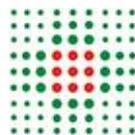


**SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA**  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



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

<b>MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO</b>		
<b>MISURA</b>	<b>Esistenti</b>	<b>Note</b>
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:		

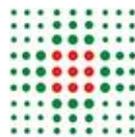


**SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA**  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



**APPENDICE**

<b>MINACCE</b>
<b>ACCESSO ILLEGITTIMO AI DATI</b>
<p><b>Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?</b></p> <p>Perdita di riservatezza dei dati personali coperti da segreto professionale; perdita del controllo dei propri dati; decifrazione non autorizzata dei dati pseudonimizzati; diffusione dei dati non autorizzata</p> <p><b>Quali sono le principali minacce che potrebbero concretizzare il rischio?</b></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; virus</p> <p><b>Quali sono le fonti di rischio?</b></p> <p>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)</p> <p><b>Quali misure fra quelle individuate contribuiscono a mitigare il rischio?</b></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><b>Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?</b></p> <p>Molto bassa: l’impatto sugli interessati potrebbe essere elevato, tuttavia le misure previste per evitare gli accessi non autorizzati rendono limitata la probabilità di accadimento</p> <p><b>Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?</b></p> <p>Molto bassa: le politiche di sicurezza informatica e le misure adottate a protezione delle postazioni di lavoro rendono quasi nulla la probabilità di accadimento</p>
<b>MODIFICHE INDESIDERATE DEI DATI</b>
<p><b>Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?</b></p> <p>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</p> <p><b>Quali sono le principali minacce che potrebbero concretizzare il rischio?</b></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; virus</p>



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



**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 rendono quasi nulla la probabilità di accadimento.

**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; 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?**

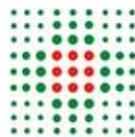
Back – up dei dati; Controllo accessi (log); Misure anti – intrusive; antivirus/firewall; Tracciabilità, Gestione postazioni; Politiche di tutela della privacy, Politiche di sicurezza informatica

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

Molto bassa: 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 rendono quasi nulla la probabilità di accadimento



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



**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	Rischio basso: $R < 7$ Rischio medio: $7 < R < 11$ Rischio alto: $R > 11$
Probabilità bassa: 2	Impatto basso: 2	
Probabilità media: 3	Impatto medio: 3	
Probabilità alta: 4	Impatto alto: 4	
Probabilità molto alta: 5	Impatto molto alto: 5	

**MATRICE DI VALUTAZIONE DEL RISCHIO**

		IMPATTO <sup>§§</sup>				
		MOLTO ALTO <sup>§</sup>	5	10	15	20
PROBABILITA'	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

<sup>§</sup> 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

<sup>§§</sup> 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 COMPLESSIVA (SOMMA COLONNA LIVELLO RISCHIO)</u>
ACCESSO ILLEGITTIMO	1*1	1	4
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