

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) PER PROGETTI DI RICERCA IN AMBITO SANITARIO SU DATI RETROSPETTIVI E PROSPETTICI

(Artt. 35 e 36 Reg. UE 2016/679; art. 110 d.lgs. 196/2003, come modificato dall'art. 44 d.l. 19/2024 conv. L. 56/2024; Provvedimento del Garante n. 298 del 9 maggio 2024)

La valutazione d'impatto sulla protezione dei dati (DPIA) consente di identificare in modo puntuale i rischi per la protezione dei dati personali connessi a un progetto di ricerca e di individuare le misure necessarie a mitigarli. Costituisce adempimento obbligatorio ai sensi dell'art. 35 del Regolamento quando il trattamento presenta un rischio elevato per i diritti e le libertà degli interessati.

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 svolto su larga scala;
- vengono trattate categorie particolari di dati (art. 9 del Regolamento);
- 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: Complicanze dell'obesità nella popolazione modenese: valutazione clinica dei pazienti afferenti all'Ambulatorio per la cura dell'Obesità dell'Unità Clinica di Endocrinologia dell'Azienda Ospedaliero-Universitaria di Modena.

Codice di Protocollo: OB-Modena — Versione 1 del 19/02/2026 (Pratica CE AVEN n. 125/2026/OSS/AOUMO).

Titolari del trattamento: le entità coinvolte si qualificano quali titolari autonomi del trattamento, ciascuna per la propria sfera:

Centro Promotore: Università degli Studi di Modena e Reggio Emilia (UNIMORE) e, per essa, il Dipartimento di Scienze Biomediche, Metaboliche e Neuroscienze, Via Pietro Giardini n. 1355, 41126 Modena (Baggiovara), C.F./P.IVA 00427620364.

Centro sperimentale: Azienda Ospedaliero-Universitaria di Modena, Ospedale Civile di Baggiovara, Dipartimento ad Attività Integrata di Medicine Specialistiche, SC Endocrinologia P.IVA: 02241740360.

Soggetto delegato: Investigatore Principale (P.I.) Prof. Vincenzo Rochira, designato delegato al trattamento da UNIMORE e autorizzato all'accesso ai dati clinici presso l'AOU di Modena

Data di compilazione: 08/07/2026.

TRATTAMENTO DEI DATI	
Descrizione del trattamento (compilare i campi successivi e allegare il modulo di fattibilità dello studio)	
Obiettivi dello studio	Obiettivo generale: integrare le attuali conoscenze al fine di migliorare la gestione diagnostico-clinica dei pazienti affetti da obesità. Obiettivo primario valutazione di una popolazione ampia e ben caratterizzata di persone che vivono con obesità al fine di: approfondire aspetti relativi alla variabilità fenotipica e del comportamento alimentare, alla tipologia di complicanze di malattia in termini di tempistica di esordio e evoluzione, valutare in real-life la risposta a lungo termine agli interventi terapeutici e infine a favorire l'elaborazione di percorsi diagnostico-terapeutici condivisi e basati sull'evidenza. Obiettivi secondari • stratificazione del rischio di complicanze mediante identificazione di predittori clinici specifici; • costituzione di una base dati aggiornata per futuri studi multicentrici.
Breve sintesi del progetto	Studio osservazionale monocentrico, retrospettivo e prospettico, basato esclusivamente sull'analisi di dati raccolti nel corso della normale pratica clinica. Non è prevista alcuna procedura interventistica né alcun esame aggiuntivo rispetto alla pratica clinica corrente. Componente retrospettiva Registrazione dei pazienti in gestione per la cura dell'obesità presso l'ambulatorio nel periodo dal 1° gennaio 2023 al 31 marzo 2026, mediante consultazione delle cartelle cliniche elettroniche presenti nel Sistema Informativo Ospedaliero (SIO) dell'AOU di Modena. Componente prospettica Arruolamento consecutivo, previo consenso informato, dei pazienti afferenti all'ambulatorio; durata 5 anni (indicativamente 1° agosto 2026 – 31 luglio 2031). Popolazione in studio: soggetti adulti (≥ 18 anni) con obesità. Stima di arruolamento: circa 2000 soggetti nel quinquennio prospettico. Durata complessiva dello studio: 60 mesi.
Tipologia di dati raccolti	
Modalità di raccolta	☒ consultazione cartelle cliniche/documentazione sanitaria (SIO) ☒ archivi di dati clinici ☒ archivi di test diagnostici ☐ dati di laboratorio ☐ altro
Trattamento dei dati (supporto)	☐ in formato cartaceo ☒ in formato digitale ☐ altro
Categorie di persone interessate	☒ Pazienti ☐ Persone sane ☐ Operatori sanitari

	☐ Soggetti vulnerabili (soggetti anziani, per età) ☐ altro
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): • storia dell'obesità (età alla diagnosi, durata, esordio, andamento, interventi pregressi); • esame obiettivo e antropometria (peso, altezza, BMI, circonferenze, indici, PA, FC, segni clinici); • esami bioumorali e ormonali; • composizione corporea e forza muscolare.
I dati personali vengono comunicati/condivisi con altri?	☐ No ☒ Sì Ambiti e natura dei dati comunicati: ☒ Promotore (UNIMORE) ☐ Dati in chiaro ☒ Dati pseudonimizzati ☐ Dati anonimi/anonimizzati ☐ altro (specificare) <i>I dati sono trasmessi dall'AOU al Promotore, quale titolare autonomo del trattamento di ricerca, esclusivamente in forma pseudonimizzata.</i> ☐ CRO ☐ altro
I dati personali vengono trasferiti all'estero?	☒ No ☐ Sì
Misure di protezione dei dati	
Verranno conservati i dati identificativi dei partecipanti?	☐ No ☒ Sì La chiave di codifica che consente il collegamento tra codice univoco e identità del paziente è conservata dal solo P.I., separatamente dai dati di studio, e non è resa pubblica. La conservazione è funzionale alle esigenze di monitoraggio e verifica da parte delle Autorità competenti, all'eventuale ripresa di contatto per la raccolta del consenso e agli obblighi documentali propri della Buona Pratica Clinica. Termine di conservazione: 7 anni dalla conclusione dello studio.
Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi o	Per non identificare direttamente l'interessato è adottata la seguente misura: ☐ adozione di tecniche crittografiche ☒ utilizzo di codici univoci per ciascun partecipante: solo il P.I. (o soggetti autorizzati) può collegare i codici all'identità dei partecipanti mediante l'uso di

<i>pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca</i>	informazioni aggiuntive, conservate separatamente e protette da misure tecniche e organizzative adeguate
--	--

PRINCIPI, FINALITÀ 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
Integrità ed esattezza	
<i>Sono state messe in campo azioni per garantire l'integrità e l'esattezza dei dati?</i>	☒ Sì ☐ No
Limitazione della conservazione	
<i>Per quanto tempo verranno conservati i dati raccolti?</i>	Indicare il numero di mesi/anni: 7 anni dalla conclusione dello studio. Decorso tale termine i dati saranno: ☐ anonimizzati completamente ☒ distrutti ☐ altro
Basi giuridiche	
<i>Quali sono le basi giuridiche del trattamento?</i>	Il trattamento si articola in due fasi, con distinte basi giuridiche. Fase retrospettiva ☒ art. 9, par. 2, lett. j) GDPR ¹ ☐ art. 110, co. 1 primo periodo Codice Privacy ² ☒ art. 110, co. 1, secondo periodo Codice Privacy ³ ☐ art. 110 bis, co. 4: Istituto di Ricerca e Cura a carattere scientifico per le attività di assistenza e ricerca dell'ambito di riconoscimento ⁴

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.

	☒ art. 6, par. 1, lett. e), GDPR ⁵ <i>Qualora i soggetti della fase retrospettiva si ripresentino a controllo, sarà loro richiesto il consenso informato alla partecipazione.</i> Fase prospettica - art. 6, par. 1, lett. a), GDPR⁶ - art. 9, par. 2, lett. a), GDPR⁷
--	---

MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO	
Informativa e consenso	
Fase prospettica	È resa informativa ai sensi degli artt. 12-13 del Regolamento ed è acquisito il consenso esplicito al trattamento dei dati, congiunto al consenso alla partecipazione allo studio.
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 per i quali non è possibile fornire l'informativa e acquisire il consenso: ☐ 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 ☒ del fatto che gli interessati risultano deceduti o non contattabili <i>Per i soggetti ricontattabili è richiesto il consenso alla prima occasione utile di controllo.</i>
Esercizio dei diritti ex artt. 15-22 del Regolamento	
È stata predisposta una procedura ad hoc da parte dell'Ente?	☒ Sì ☐ No

A CURA DELL'UNIVERSITÀ

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO		
MISURA	Esisten ti	Note
Organigramma interno	X	Predisposto con regolamento interno.
Nomine responsabili esterni	X	Nel caso di specie non sono predisposte; l'Università è dotata di template.

[Indr: 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]

⁵ Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

⁶ L'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità.

⁷ L'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui all'art. 9 paragrafo 1.

Nomina DPO	X	Contratto Rep. n. 10/2025; atto di designazione del 16.7.2025 - prot. n. 211401 - rep. nr. 726/2025
Informativa	X	Nel caso di specie, per la parte di studio retrospettivo non è possibile fornire l'informativa all'interessato. Ordinariamente il titolare predispone informative per ogni trattamento realizzato. Nella fase prospettica l'informativa è resa e il consenso acquisito.
Istruzioni persone autorizzate al trattamento	X	Il personale coinvolto riceve adeguate istruzioni in sede di incarico e mediante le policy adottate dal titolare.
Formazione	X	Il personale coinvolto è sensibilizzato e formato in materia di data protection.
Registri	X	Il titolare ha predisposto i registri dei trattamenti ai sensi dell'art. 30 GDPR e delle Linee guida CODAU.
Procedure	X	Il titolare ha adottato le procedure necessarie a garantire un'adeguata <i>compliance</i> GDPR.
Politiche di tutela della privacy	X	L'attività del titolare è orientata ad una strutturata compliance GDPR: > designato DPO esterno con il quale intercorre uno stretto confronto; > adottate misure tecniche ed organizzative; > implementate misure tecniche di sicurezza ICT richieste da AGID; > adottati regolamenti e procedure interni in materia di data protection.
Distruzione/smaltimento sicuro cartaceo		Non applicabile nel caso di specie (trattamento esclusivamente digitale).
Inventario degli asset	X	• <u>Inventario dei dispositivi autorizzati e non autorizzati</u>: Sono gestiti attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia permesso solo ai dispositivi autorizzati e che i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso. Sono adottate misure per ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni, portatili, periferiche, dispositivi, supporti removibili ecc.) siano utilizzate per danneggiare dati personali. • <u>Inventario dei software autorizzati e non autorizzati</u>: Sono gestiti attivamente tutti i software sulla rete in modo che sia installato ed eseguito solo il software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione. Sono adottate misure per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni, software ecc.) vengano sfruttate per danneggiare i dati personali trattati. Si tratta di: aggiornamenti, protezione fisica e accessi, lavoro su spazio di rete protetto, controlli di integrità, logging ecc.

Misure anti-intrusive (cartelli di divieto di accesso ai locali, strumenti per la rilevazione degli accessi, guardiana, portineria, serrature armadi, schedari, ecc.)	X	• Sono adottate misure per il controllo degli accessi fisici agli uffici universitari, nonché ai "locali strategici" (es. locali server, locali pc, archivi). • Sono implementati sistemi di protezione adeguati volti a garantire la sicurezza della rete (es. firewall e antivirus).
Politiche di sicurezza informatica	X	• Istituita, implementata e gestita attivamente (tracciata, segnalata, corretta) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni. • Acquisite, valutate e intraprese continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.
Controllo accessi (log)	X	• Sono adottati Regolamenti e Procedure per la gestione degli incarichi al trattamento del personale, nonché delle relative credenziali di accesso ai sistemi/file autorizzati. • Sono adottate regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.
Antivirus / firewall	X	• Sono implementati sistemi di protezione adeguati volti a garantire la sicurezza della rete (es. firewall e antivirus). • Sono adottate misure volte a proteggere l'accesso alla rete, le postazioni ed i server contro malware che potrebbero compromettere la sicurezza dei dati personali trattati.
Politiche di clear screen		Non applicabile nel caso di specie.
Back-up dei dati	X	• L'università adotta politiche di backup tali da assicurare la disponibilità e l'integrità dei dati personali. • Come richiesto da AGID, sono adottate procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.
Politiche di trasmissione dei dati	X	I dati sono trasmessi dall'AOU al Promotore esclusivamente in forma pseudonimizzata.
nel caso si utilizzi un sito web esterno:		Non applicabile nel caso di specie.
Connessione sicura		
Accesso protetto da utenza personale		
Crittografia		__no__

Anonimizzazione		__no__
Pseudonimizzazione	X	Sì. Codice univoco per ciascun partecipante; chiave conservata dal solo P.I., separatamente.
Sicurezza dei documenti cartacei		Non applicabile nel caso di specie.
Gestione postazioni	X	Le postazioni sono accessibili ai soli utenti universitari. È adottato un regolamento sul corretto utilizzo delle postazioni informatiche.
Autenticazione	X	Sono creati, affidati e gestiti diversi profili utente in virtù delle mansioni svolte. In particolare, ogni utente dei sistemi del titolare è dotato di un User e di una password creata nel rispetto dei regolamenti interni.
Policy di gestione data breach	X	• Sono adottate adeguate procedure di gestione dei data breach; • In via preventiva sono acquisite, valutate e intraprese continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.
Minimizzazione	X	Il processo di trattamento dei dati effettuato nel progetto è tarato sui soli dati considerati necessari al raggiungimento degli obiettivi della ricerca. Ciò in considerazione: • della selezione "by design" a monte dei soli dati effettivamente pertinenti ed adeguati al raggiungimento delle finalità del progetto. • della limitazione dell'accesso ai dati; • della realizzazione delle attività di ricerca su un data set pseudonimizzato.

APPENDICE

La valutazione d'impatto di seguito operata prende le mosse dalle misure ordinariamente adottate da UNIMORE con riferimento agli Studi Clinici nei quali i dati sono trattati nei sistemi universitari. Poiché i dati di origine risiedono nel Sistema Informatico Ospedaliero e su postazioni del personale medico dell'AOU di Modena, la presente valutazione è suscettibile di integrazione con le specifiche misure di sicurezza adottate dall'AOU con riferimento ai propri sistemi.

ACCESSO ILLEGITTIMO AI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Perdita di riservatezza dei dati personali; perdita del controllo dei propri dati; indebita divulgazione o utilizzo non autorizzato di dati pseudonimizzati; re-identificazione non autorizzata mediante accesso alla chiave di codifica. Data la presenza di categorie particolari ad elevata delicatezza (salute psichica, vita sessuale), l'impatto potenziale sull'interessato è qualitativamente rilevante.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Utilizzo inappropriato o sottrazione (phishing, malware) delle credenziali di accesso ai sistemi e al database pseudonimizzato; abuso dei privilegi da parte di operatori abilitati; attacchi informatici (intrusioni, malware,

ransomware); errata profilazione degli utenti; accesso non autorizzato alla chiave di codifica custodita dal P.I.

Quali sono le fonti di rischio?

Fonti umane interne: comportamenti non conformi alle procedure. Fonti umane esterne: attacchi informatici di terzi non autorizzati. Fonti non umane: malware, vulnerabilità software, bug introdotti da aggiornamenti.

Quali misure contribuiscono a mitigare il rischio?

Pseudonimizzazione mediante codice univoco, con chiave custodita separatamente dal solo P.I.; istruzioni agli autorizzati; formazione; procedure e policy; misure anti-intrusive; politiche di sicurezza informatica; controllo accessi (log); antivirus/firewall; autenticazione; gestione delle postazioni; misure ICT minime richieste da AgID sui sistemi UNIMORE e AOU. I dati risiedono su computer ad accesso esclusivo del personale medico, protetti da username e password.

Come stimereste la gravità del rischio?

La gravità è stimata **Bassa**. L'impatto potenziale è oggettivamente elevato per la natura dei dati; tuttavia la pseudonimizzazione e le misure adottate rendono estremamente limitata la probabilità che un accesso illegittimo consenta l'identificazione degli interessati.

Come stimereste la probabilità del rischio?

La probabilità è **Molto bassa**. Chi accedesse al solo dataset pseudonimizzato, privo della chiave custodita dal P.I., disporrebbe di informazioni non riferibili a persone identificate o identificabili: non si integrerebbe un accesso a dati personali identificativi. Anche in scenari più complessi (accesso simultaneo a dataset e chiave) la probabilità resta trascurabile, in ragione della custodia separata della chiave e delle misure ICT adottate.

MODIFICHE INDESIDERATE DEI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Perdita di integrità del dataset, con compromissione della qualità e affidabilità della ricerca. L'impatto principale riguarda l'affidabilità scientifica dello studio e non i diritti degli interessati: la fonte originaria (cartella clinica AOU) resta intatta, distinta e non collegata al dataset pseudonimizzato.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Utilizzo inappropriato o sottrazione delle credenziali; abuso dei privilegi; attacco informatico; errata profilazione degli utenti; accesso non autorizzato; virus.

Quali sono le fonti di rischio?

Fonti umane interne: comportamenti non conformi alle procedure. Fonti umane esterne: attacchi informatici di terzi. Fonti non umane: malware, vulnerabilità software, bug da aggiornamenti.

Quali misure contribuiscono a mitigare il rischio?

Limitazione dell'accesso ai file ai soli profili autorizzati; istruzioni agli autorizzati; formazione; procedure e policy; misure anti-intrusive; politiche di sicurezza informatica; controllo accessi (log); antivirus/firewall; backup; gestione delle postazioni; autenticazione.

Come stimereste la gravità del rischio?

La gravità è **Molto bassa**. Lo studio opera su un dataset pseudonimizzato estratto dalla cartella clinica AOU, che resta intatta e non collegata; una modifica indesiderata del dataset di studio non avrebbe impatti sostanziali sui diritti dei pazienti.

Come stimereste la probabilità del rischio?

La probabilità è **Molto bassa**. Sono adottate misure ICT aggiornate, controllo degli accessi fisici e logici, backup periodici; le procedure UNIMORE e AOU sono integrate dagli iter definiti ad hoc per lo studio.

PERDITA DI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Un'eventuale perdita riguarderebbe esclusivamente dati informatici pseudonimizzati. Potrebbe determinare un impatto limitato sull'operatività dello studio (rallentamento temporaneo), ma non rischi significativi per i diritti e le libertà degli interessati: il dataset è pseudonimizzato e non consente l'identificazione, e l'Università adotta procedure di backup e ripristino conformi alle indicazioni AgID.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minacce di natura informatica: distruzione, cancellazione o corruzione del file (ransomware, guasti hardware, malfunzionamenti). Errori umani (cancellazione accidentale, malware da posta elettronica) o eventi naturali (incendio, allagamento) che danneggino il datacenter.

Quali sono le fonti di rischio?

Fonti umane interne: operatori che, per errore, cancellano o sovrascrivono dati. Fonti umane esterne: attacchi informatici. Fonti non umane: virus, calamità naturali, guasti tecnici.

Quali misure contribuiscono a mitigare il rischio?

Backup periodici; controllo degli accessi (log); antivirus e firewall; misure anti-intrusione; tracciabilità delle operazioni; gestione sicura delle postazioni; formazione e istruzioni agli autorizzati; politiche di sicurezza informatica.

Come stimereste la gravità del rischio?

La gravità è **Molto bassa**. La perdita del dataset pseudonimizzato non inciderebbe sui diritti degli interessati (dato non identificante) e non pregiudicherebbe la ricerca, grazie alle procedure di backup e ripristino conformi ad AgID; la fonte originaria dei dati non è mai coinvolta.

Come stimereste la probabilità del rischio?

La probabilità è **Molto bassa**. Le misure tecniche e organizzative rendono altamente improbabile la perdita; in ogni caso essa non sarebbe definitiva, potendo il file essere ripristinato dalle copie di backup.

PROBABILITA' (P)	IMPATTO (I)	RISCHIO (R=P*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	

A CURA DEL DPO
MATRICE DI VALUTAZIONE DEL RISCHIO

		IMPATTO ^{SS}				
PROBABILITA'	MOLTO ALTO^S	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
--	------------------------	--------------	--------------	-------------	-----------------------

^s 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

^{ss} 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</u>
ACCESSO ILLEGITTIMO	1*2	2	4
MODIFICHE INDESIDERATE DEI DATI	1*1	1	
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

Esito complessivo della valutazione

Il rischio residuo complessivo per i diritti e le libertà degli interessati è valutato **Basso**. La pseudonimizzazione con custodia separata della chiave, la permanenza intatta della fonte clinica originaria presso l'AOU e le misure tecniche e organizzative adottate (integrate dalle misure ICT dell'AOU) riducono la probabilità di concretizzazione delle minacce a livelli molto bassi.

Non ricorrono i presupposti per la consultazione preventiva del Garante ai sensi dell'art. 36 del Regolamento, adempimento peraltro non più previsto dall'art. 110 del Codice — come modificato dall'art. 44 del d.l. 19/2024 conv. L. 56/2024 — per i trattamenti di ricerca sanitaria in assenza di consenso.