

VALUTAZIONE D'IMPATTO PRIVACY (DPIA)

CONTESTO DEL TRATTAMENTO OGGETTO DI VALUTAZIONE D'IMPATTO

Visione d'insieme

Presentazione del(dei) trattamento(i) considerato(i)

Descrizione del trattamento	Tumor segmentation from whole-body [18F]fluorodeoxyglucose PET/CT images with Convolutional Neural Network (CNN)
Titolare del trattamento	Azienda tutela della salute Liguria (ATS Liguria) con sede in piazza della Vittoria, 15 - 16121 Genova (pec: protocollo@pec.atsliguria.it / e-mail: protocollo@atsliguria.it) – Area Sociosanitaria Locale 5
Referenti interni/strutture interne coinvolti	Prof. Andrea Ciarmiello - S.C. Medicina Nucleare Ospedale S. Andrea Via Vittorio Veneto 197 La Spezia
Eventuali responsabili esterni	Nessuno
Eventuali sub-responsabili (specificare di quale responsabile)	Nessuno
Eventuali contitolari del trattamento	Nessuno

STUDIO DEI PRINCIPI FONDAMENTALI

Valutazione delle misure poste a garanzia della proporzionalità e necessità del trattamento

Precisare la finalità perseguita e indicare gli elementi che rendono legittimo perseguirla

Finalità	Legittimità
Studio osservazionale retrospettivo non randomizzato con lo scopo di valutare l'associazione tra le lesioni segmentate dal modello AI e quelle segmentate manualmente in pazienti con tumore del polmone, linfomi, melanomi, mammella. I pazienti verranno reclutati retrospettivamente tra quelli sottoposti a [¹⁸F]FDG-PET/TC dal 01.2019 al 12.2025.	Finalità di ricerca. Il trattamento dei dati personali necessario per la realizzazione dello studio ha come base giuridica il consenso ai sensi degli artt. 6 par. 1 lett. a) e 9 par. 2 lett. a) del GDPR.

Dati, destinatari, pertinenza, minimizzazione e durata della conservazione

Descrizione delle tipologie di dati oggetto di trattamento (C= comuni / S= categorie particolari / G= giudiziari), fonte di provenienza ed eventuali destinatari esterni, applicazione del principio della “minimizzazione” dei dati trattati (i dati devono essere adeguati, pertinenti, non eccedenti rispetto alle finalità perseguite), durata della conservazione prevista

	Dettaglio dei dati trattati	Tipo di dati (C/S/G)	Fonte di provenienza dei dati	Eventuali destinatari esterni	Giustificazione della pertinenza dei dati rispetto alle finalità	Misure di minimizzazione	Durata della conservazione	Giustificazione della durata della conservazione	Modalità di distruzione al termine della conservazione
1	Accession number	C	PACS	Nessuno	Necessità di avere campione rappresentativo	Estrazione del solo set di dati necessario allo studio; rimozione degli identificativi diretti e dei metadati DICOM non necessari; sostituzione degli identificativi con un codice alfanumerico casuale; conservazione separata e ad accesso ristretto della chiave di collegamento; accesso al dataset limitato al personale	15 anni	Necessità di avere adeguato potere statistico	Eliminazione per cancellazione sicura secondo le procedure aziendali
2	Età	C	PACS	Nessuno	Necessità di avere campione rappresentativo		15 anni	Necessità di avere adeguato potere statistico	Eliminazione per cancellazione sicura secondo le procedure aziendali
3	Sesso	C	PACS	Nessuno	Necessità di avere campione rappresentativo		15 anni	Necessità di avere adeguato potere statistico	Eliminazione per cancellazione sicura secondo le procedure aziendali
4	Peso	C	PACS	Nessuno	Necessità di avere campione rappresentativo		15 anni	Necessità di avere adeguato potere statistico	Eliminazione per cancellazione sicura secondo le procedure aziendali
5	Altezza	C	PACS	Nessuno	Necessità di avere campione rappresentativo		15 anni	Necessità di avere adeguato potere statistico	Eliminazione per cancellazione sicura secondo le procedure aziendali
6	Dose somministrata	C	PACS	Nessuno	Necessità di avere campione rappresentativo		15 anni	Necessità di avere adeguato potere statistico	Eliminazione per cancellazione sicura secondo le procedure aziendali

	Dettaglio dei dati trattati	Tipo di dati (C/S/G)	Fonte di provenienza dei dati	Eventuali destinatari esterni	Giustificazione della pertinenza dei dati rispetto alle finalità	Misure di minimizzazione	Durata della conservazione	Giustificazione della durata della conservazione	Modalità di distruzione al termine della conservazione
7	Immagini PET	S	PACS	Nessuno	Necessità di avere campione rappresentativo	Estrazione del solo set di dati necessario allo studio; rimozione degli identificativi diretti e dei metadati DICOM non necessari; sostituzione degli identificativi con un codice alfanumerico casuale;	15 anni	Necessità di avere adeguato potere statistico	Eliminazione per cancellazione sicura secondo le procedure aziendali
8	Immagini TAC	S	PACS	Nessuno	Necessità di avere campione rappresentativo	conservazione separata e ad accesso ristretto della chiave di collegamento; accesso al dataset limitato al personale autorizzato	15 anni	Necessità di avere adeguato potere statistico	Eliminazione per cancellazione sicura secondo le procedure aziendali

Chiarire come si dimostra che i dati oggetto di trattamento sono sempre esatti e aggiornati

Misure per garantire la qualità dei dati

I dati anagrafici, quelli relativi alla salute vengono raccolti dal paziente, dalla sua cartella clinica e dai referti clinici. L'interessato gode sempre del diritto di richiedere l'aggiornamento di eventuali dati divenuti obsoleti o errati rivolgendosi allo sperimentatore ovvero al Responsabile Protezione Dati dell'Azienda.

Base giuridica del trattamento

Barrare la/le voce/i che interessa/interessano per i dati comuni.

Per i DATI "COMUNI" (es. anagrafiche, numero di telefono, indirizzo e-mail)	
☒	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità
☐	il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso
☐	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento PRECISARE LA FONTE NORMATIVA DELL'OBBLIGO:
☐	il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica
☐	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 PRECISARE QUALE:

Barrare la/le voce/i che interessa/interessano per le categorie particolari di dati.

Per le CATEGORIE PARTICOLARI DI DATI (es. stato di salute, orientamento sessuale, dati genetici, orientamento religioso, ecc.)	
☒	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche Per i soli casi per cui non sia possibile ottenere il consenso degli interessati ci si atterrà a quanto previsto dell'art. 110 D.Lgs. 196/2003 e s.m.i.
☐	il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo
☐	il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso
☐	il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato
☐	il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali
☐	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato PRECISARE QUALE:
☐	il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità
☐	il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale
☐	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
☐	ricorre l'ipotesi di esenzione del consenso per gli studi clinici ex art. 110 D.Lgs. 196/2003 e s.m.i.

Valutazione delle misure a protezione dei diritti personali degli interessati

Determinazione e descrizione delle misure adottate per fornire l'informativa agli interessati di cui agli artt. 13 e 14 GDPR.

Misure per garantire il diritto all'informativa	Giustificazione dell'eventuale esenzione
I pazienti potenzialmente eleggibili saranno preventivamente informati delle caratteristiche dello studio, dei loro diritti, dell'assenza di rischi e anche dell'assenza di benefici attraverso due informative con consenso informato. La prima informativa con consenso è studio specifica: riporta le caratteristiche e le finalità dello studio, le tempistiche della ricerca, gli impegni che dovrà affrontare il paziente, il Comitato Etico che lo ha valutato, i contatti dei ricercatori, i diritti e le tutele del paziente nel partecipare alla ricerca clinica in accordo alle Norme di Buona Pratica Clinica e alla normativa vigente sugli studi clinici. La seconda informativa con consenso riguarda il trattamento dei dati personali del paziente. Tale informativa riporta tutti i diritti del paziente in ambito di privacy, il titolare del trattamento dei dati con i relativi recapiti, il contatto del DPO, le modalità per esercitare i propri diritti, la tipologia di dati raccolti, la durata della loro conservazione oltre ad informazioni generali sulla privacy. Nella somministrazione dei consensi ai potenziali pazienti verrà dato tutto il tempo necessario per porre eventuali domande e per decidere se partecipare alla ricerca, saranno inoltre informati sul loro diritto di ritirare i consensi in qualsiasi momento. I pazienti eleggibili che desiderano aderire allo studio dovranno firmare entrambi i consensi che saranno controfirmati dal medico ricercatore che ha somministrato le informative. Una copia dei consensi firmata viene rilasciata al paziente e gli originali vengono conservati nella documentazione dello studio. Ove applicabile le informative saranno proposte al legale rappresentate, qualora decadano le motivazioni per il tutoraggio, l'informativa sarà somministrata direttamente al paziente che potrà decidere in autonomia se continuare o terminare la partecipazione allo studio. In caso il paziente decida di uscire dallo studio i dati raccolti fino a quel momento saranno conservati per non inficiare i risultati della ricerca ma non verranno raccolti ulteriori dati.	Nessuna

Determinazione e descrizione delle misure per raccogliere il consenso (se applicabile).

Misure per la raccolta del consenso	Giustificazione dell'eventuale impossibilità della loro messa in opera
Come sopra	Nessuna, in caso di incapacità del partecipante a fornire il consenso, lo stesso sarà acquisito dal legale rappresentante.

Determinazione e descrizione delle misure per l'esercizio dei diritti di cui al GDPR (ARTT. 15 E SS.)

Indicare i diritti applicabili al trattamento in questione
ACCESSO (art. 15)
RETTIFICA (art. 16)
CANCELLAZIONE/OBLIO (art. 17)
LIMITAZIONE DEL TRATTAMENTO (art. 18)
NOTIFICA IN CASO DI RETTIFICA/CANCELLAZIONE E/O LIMITAZIONE (art. 19)
PORTABILITÀ (art. 20)
OPPOSIZIONE (art. 21)
NON ESSERE SOTTOPOSTO A UNA DECISIONE BASATA UNICAMENTE SUL TRATTAMENTO AUTOMATIZZATO, COMPRESA LA PROFILAZIONE (art. 22)

Se rispetto al trattamento in questione non possono essere esercitati uno o più diritti, motivarlo:

Giustificazione
Nessuna

Gestione del riscontro agli interessati che esercitano un diritto.

Modalità prevista per la risposta agli interessati che esercitano un diritto:
Il riscontro viene fornito direttamente dal Responsabile Protezione Dati (DPO) dell'Azienda

Trasferimento extra-UE dei dati

Determinazione e descrizione delle misure per l'eventuale trasferimento dei dati al di fuori dell'Unione Europea

Tipologia di dati oggetto di trasferimento	Motivazione del trasferimento	Soggetto destinatario	Paese destinatario	Legittimante del trasferimento (decisione di adeguatezza, clausole contrattuali tipo, regole vincolanti di impresa, altre misure di cui all'art. 49 GDPR fra cui consenso, ecc.)
Nessuno				

MISURE DI SICUREZZA

Valutazione delle misure di sicurezza

Descrizione e valutazione delle misure che contribuiscono a contenere i rischi legati alla sicurezza dei dati (art. 32) circa l'intera attività di trattamento:

Misure specifiche applicate sui dati trattati	Modalità operative
Cifratura/Pseudonimizzazione	codice alfanumerico randomizzato
Controllo degli accessi logici	accessi personali mediante password
Tracciabilità degli accessi	gli accessi informatici ai sistemi aziendali sono soggetti a logging
Archiviazione sicura dei dati	mediante password in server aziendali

Nel caso di trattamenti svolti per mezzo di uno specifico software

	Per la segmentazione manuale delle immagini sono impiegati NORA e PETVCAR su Advantage Workstation; il modello di segmentazione è implementato mediante i framework MONAI e nnU-Net; le analisi statistiche sono svolte mediante RStudio. Tutti gli applicativi sono installati o eseguiti localmente su infrastruttura aziendale. I dati e gli output restano conservati su server aziendali e non sono previste funzioni cloud, trasmissioni di dati, accessi remoti o accessi ai dati da parte dei fornitori
Denominazione software	NORA medical imaging platform
Fornitore del software	Università di Friburgo, Germania
Descrizione sintetica attività gestita	Nora è un framework basato sul web per l'analisi di immagini mediche. E' usato come interfaccia web di alto livello, accessibile da qualsiasi browser, per visualizzare, organizzare, elaborare e condividere dati in modo altamente personalizzabile. l'istanza di Nora può essere eseguita tramite un'installazione locale presso il proprio istituto.
Tecnologia	Open-source piattaforma di analisi delle immagini
Base dati	in server aziendali

Denominazione software	PETVCAR - PET Volume Computerized Assisted Reporting
Fornitore del software	Ge Healthcare
Descrizione sintetica attività gestita	Confronto multimodale e tra esami multipli per valutare l'attività metabolica delle lesioni nel corso del tempo. PET VCAR semplifica la valutazione dei dati metabolici, offrendo la possibilità di interpretare, quantificare e gestire i dataset PET/CT in modo più efficiente. PET VCAR (Volume Computer Assisted Reading) migliora la visualizzazione e il monitoraggio analitico della progressione della malattia o della risposta alla terapia. Consente di calcolare diversi valori SUV (Standard Uptake Value), di misurare l'attività metabolica e il volume delle aree di attività individuate alla PET, nonché di confrontare esami TC, PET/CT e RM per valutazioni basali e di follow-up.
Tecnologia	piattaforma per analisi delle immagini
Base dati	in server aziendali

Denominazione software	Modello di rete MONAI (Medical Open Network for Artificial Intelligence)
Fornitore del software	MONAI Consortium
Descrizione sintetica attività gestita	MONAI (Medical Open Network for AI) è un programma aperto creato per aiutare i computer a capire le immagini mediche, come TAC e risonanze magnetiche. Funziona come un maestro esperto che insegna all'intelligenza artificiale a riconoscere organi o malattie, come un tumore, analizzando milioni di esempi passati. Il sistema lavora in tre passi principali: 1) Preparazione (MONAI Label): I medici usano l'intelligenza artificiale per cerchiare o evidenziare velocemente le parti malate nelle immagini. Questo serve ad "insegnare" al computer cosa deve cercare. 2) Studio (MONAI Core): Il programma usa questi esempi per imparare. Si basa su PyTorch (un motore molto famoso per l'intelligenza artificiale) ed è ottimizzato per processare immagini 3D pesanti. 3) Uso pratico (MONAI Deploy): Una volta che il programma ha imparato, i medici possono usarlo negli ospedali per analizzare nuove immagini in modo automatico e veloce.
Tecnologia	Open-source framework for healthcare imaging AI
Base dati	in server aziendali

Dati trattati dal software nel contesto di utilizzo

Tipologie dei dati gestiti mediante il prodotto software	Sì	No	N.A.
Il software gestisce dati Personali	X		
Il software gestisce categorie particolari di dati personali	X		
Il software gestisce dati relativi a condanne penali e reati			X
Il software gestisce dati a maggior tutela di anonimato (HIV, IVG, ecc...)		X	
Ambito di gestione del dato	Sì	No	N.A.
Sono gestiti dati relativi a episodi di cura	X		
Sono gestiti dati relativi a pazienti	X		
Sono gestiti dati relativi a dipendenti (in quanto dipendenti dell'Azienda utilizzatrice)		X	
Sono gestiti dati relativi a fornitori		X	
Sono conservati nel sistema documenti (esempio: PDF) che contengono dati personali e categorie particolari di dati personali e/o dati relativi a condanne penali o reati riferiti all'interessato (dati non disaccoppiabili)	X		
Rispetto delle misure di sicurezza	Sì	No	N.A.
Il software è integrato con sistemi di sicurezza permettendo la conformità al GDPR necessarie per lo scenario d'impiego cui è destinato: Privacy by design; Privacy by default; minimizzazione; pseudonimizzazione.			X
Oppure: Il software è parzialmente integrato con sistemi di sicurezza. Tuttavia, è possibile sviluppare dei controlli compensativi che permettono la conformità al GDPR necessarie per lo scenario di impiego cui è destinato.			X
Il software permette l'autenticazione degli utenti basata su tecniche di strong authentication (autenticazione basata su password ed OPT)			X
Oppure: Il software permette l'autenticazione degli utenti tramite smart card (CNS, ecc.)			X
Sono previste per default tecniche di abilitazione automatica di meccanismi di costruzione di password complesse			X

Misure di sicurezza del software nel contesto di utilizzo

Misure minime	Sì	No	N.A.
La componente privata delle credenziali di accesso è di almeno 8 caratteri alfanumerici	X		
È prevista l'obbligatorietà del cambio password al primo accesso	X		
È prevista la modifica obbligatoria della password ogni 3 / 6 mesi	X		
È prevista la disattivazione automatica della password dopo 6 mesi di non utilizzo	X		
È prevista la disconnessione dell'utente in caso di non uso dell'applicativo per un periodo di tempo parametrizzabile	X		
Il software tiene traccia (log accessi e log attività) delle operazioni effettuate tramite applicativo, comprese le attività di sola visualizzazione dei dati, per un tempo parametrizzabile.	X		
Il software permette la profilazione degli utenti (dipendenti autorizzati ad istruire le pratiche e quindi al trattamento dei relativi dati personali) in modo granulare da consentire solo la visibilità necessaria al ruolo svolto.	X		
Rispetto delle misure e degli accorgimenti in tema di amministratori di sistema	Sì	No	N.A.
È prevista la possibilità di creare livelli differenziati di amministrazione del sistema	X		
È previsto un sistema di registrazione (access log) per gli accessi logici degli amministratori di sistema al database di supporto dell'applicativo	X		
Il sistema di access log ha caratteristiche di inalterabilità, completezza e di verifica della integrità dello stesso	X		
L'access log contiene almeno i riferimenti temporali, la descrizione dell'evento che le ha generate, l'identificazione del soggetto che ha compiuto l'accesso	X		
L'access log è conservato in maniera inalterabile per almeno sei mesi	X		

Misure di sicurezza e cancellazione dal software nel contesto di utilizzo

Misure specifiche per categorie particolari di dati personali o dati personali relativi a condanne penali e reati	Sì	No	N.A.
I dati idonei a rivelare lo stato di salute e la vita sessuale/orientamento sessuale sono registrati e conservati separatamente dagli altri dati personali soggetti a trattamenti che non richiedono il loro utilizzo (disaccoppiamento)		X	
Il software consente l'adozione di tecniche di cifratura o di codici identificativi che non esplicitano direttamente il contenuto informativo in relazione alla gestione di dati idonei a rivelare lo stato di salute o la vita sessuale/orientamento sessuale.			X
Il software consente l'adozione di tecniche di pseudonimizzazione in relazione alla gestione di categorie particolari di dati personali, o dati personali relativi a condanne penali o reati			X
Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, sono trattati mediante codici identificativi che non esplicitano direttamente il contenuto informativo		X	
Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, o documenti che contengono in modo non divisibile dati personali e categorie particolari di dati personali sono trattati mediante tecniche di cifratura		X	
Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, sono trattati mediante altre soluzioni rispetto alle due precedenti, ai fini della loro temporanea inintelligibilità	X		
Cancellazione dei dati	Sì	No	N.A.
Il sistema consente di definire, per classi di informazioni, il tempo di conservazione in relazione al momento in cui sono state prodotte e al momento in cui è stata raggiunta la finalità per le quali sono state raccolte.	X		
Il sistema consente la cancellazione delle informazioni che hanno raggiunto il tempo limite di conservazione	X		
Il sistema consente di individuare le informazioni relative ad un soggetto (interessato), e in modo puntuale settarle per la cancellazione, il blocco, e l'eventuale ripristino a seguito di blocco	X		
Il sistema dispone di servizi (esempio in collaborazione applicativa) che consentono ad un sistema esterno di individuare le informazioni relative ad un soggetto (interessato), e in modo puntuale settarle per la cancellazione, il blocco, e l'eventuale ripristino a seguito di blocco			X

ANALISI DEI RISCHI

Preparazione degli elementi utili alla validazione

Elaborazione della sintesi relativa alla conformità al GDPR delle misure che consentono il rispetto dei principi fondamentali

Legenda qualità delle misure applicate

0	1	2	3
Non applicabile	Non soddisfacente	Migliorabile	Soddisfacente

Misure di carattere legale che non incidono sulla probabilità del rischio.

Misure che consentono il rispetto dei principi fondamentali	Valutazione	Eventuali misure correttive previste
Finalità: determinate, esplicite e legittime	3	
Base giuridica	3	
Minimizzazione dei dati: adeguati, pertinenti e limitati (necessari)	3	
Qualità dei dati: esatti ed aggiornati	3	
Durata della conservazione	3	
Misure a protezione dei diritti degli interessati	Valutazione	Eventuali misure correttive previste
Informazione agli interessati (trattamento legale e trasparente)	3	
Raccolta del consenso	3	
Esercizio dei diritti di cui al GDPR	3	
Sub responsabili: identificati e contrattualizzati	0	
Trasferimento dei dati extra-UE nel rispetto del GDPR	0	
Pseudonimizzazione dei dati trattati	3	

Misure tecniche e organizzative di sicurezza che incidono sulla probabilità del rischio.

Misure riguardanti i dati oggetto di trattamento	Valutazione			Eventuali misure correttive previste
	Accesso illegittimo ai dati	Modifica non desiderata dei dati	Perdita dei dati	
Cifratura/Pseudonimizzazione dei dati trattati	3	3	3	
Tracciabilità delle operazioni sui dati	3	3	3	
Archiviazione sicura dei dati	3	3	3	
Misure generali di sicurezza del sistema dove il trattamento è effettuato	Valutazione			Eventuali misure correttive previste
	Accesso illegittimo ai dati	Modifica non desiderata dei dati	Perdita dei dati	
Continuità operativa (piano di continuità operativa per i dati trattati)	3	3	3	3
Protezione da attacchi informatici (utilizzo di antivirus, antimalware, intrusion prevention system)	3	3	3	3
Gestione delle postazioni lavoro (blocco della postazione quando non presidiata)	3	3	3	3
Sicurezza dei siti web e sicurezza dei canali informatici utilizzati (protocollo https, firewall, VPN)	3	3	3	3
Back-up e disaster recovery	3	3	3	3
Modalità di mantenimento server/sistemi/software (aggiornamento del software, del sistema operativo e dell'hardware)	3	3	3	3
Controllo degli accessi informatici dove sono trattati i dati (autenticazione e profilazione utenti)	3	3	3	3
Controlli degli accessi fisici ai locali dove sono trattati i dati	3	3	3	3
Prevista cifratura dei dischi rigidi di server e/o postazioni	3	3	3	3
Distruzione sicura dell'hardware	3	3	3	3

Misure riguardanti i dati oggetto di trattamento	Valutazione			Eventuali misure correttive previste
	Accesso illegittimo ai dati	Modifica non desiderata dei dati	Perdita dei dati	
Misure generali di sicurezza del sistema dove il trattamento è effettuato	Accesso illegittimo ai dati	Modifica non desiderata dei dati	Perdita dei dati	Eventuali misure correttive previste
Organizzazione (il titolare del trattamento ha realizzato e mantiene un'organizzazione interna dei ruoli e delle responsabilità nel trattamento dati personali)	3	3	3	3
Gestione delle regole (il titolare del trattamento ha realizzato e applica politiche interne in materia di protezione dati personali)	3	3	3	3
Gestione dei rischi (il titolare del trattamento applica i principi di privacy by design e by default e svolge valutazioni del rischio in riferimento ai trattamenti effettuati)	3	3	3	3
Gestione del progetto (il trattamento oggetto della presente valutazione è condotto mediante la chiara definizione dei ruoli, delle responsabilità, delle finalità e delle modalità di svolgimento da parte del titolare del trattamento)	3	3	3	3
Gestione degli incidenti e della violazione dei dati (il titolare del trattamento ha realizzato e applica una procedura interna in materia di data breach)	3	3	3	3
Gestione del personale (il titolare del trattamento individua al proprio interno le persone autorizzate e le sottopone a formazione periodica in materia di privacy)	3	3	3	3
Rapporti con i terzi (il titolare del trattamento provvede all'individuazione dei ruoli privacy ricoperti da eventuali soggetti esterni con cui si rapporta, alla stipula degli eventuali accordi di contitolarità e alla nomina dei responsabili ove necessario)	0	0	0	0

Misure riguardanti i dati oggetto di trattamento	Valutazione			Eventuali misure correttive previste
	Accesso illegittimo ai dati	Modifica non desiderata dei dati	Perdita dei dati	
Supervisione e audit (il titolare del trattamento effettua periodicamente verifiche interne e sui responsabili esterni in tema di <i>compliance</i> con la normativa in materia di privacy).	3	3	3	3

	Valutazione		
	Accesso illegittimo ai dati	Modifica non desiderata dei dati	Perdita dei dati
Numero occorrenze valutazione 3	29	29	29
Numero occorrenze valutazione 2	0	0	0
Numero occorrenze valutazione 1	0	0	0
Numero occorrenze valutazione 0	3	3	3

VALUTAZIONE DEL RISCHIO (a cura dell'ufficio privacy)

Probabilità del rischio percentuale

0 – 25	Molto Alta	26-50	Alta	51-75	Media	75-100	Bassa
--------	------------	-------	------	-------	-------	--------	-------

Valutare la probabilità che l'impatto individuato si verifichi in base al valore totale della precedente tabella.

Probabilità (P)	Descrizione della probabilità	Valore
Bassa	La minaccia / rischio non si può realizzare	1
Media	È probabile che la minaccia / rischio si realizzi	2
Alta	La minaccia / rischio si verificherà sicuramente prima o poi	3
Molto alta	La minaccia si realizzerà con certezza nel prossimo futuro	4

Per garantire una corretta valutazione di seguito vengono riportati gli impatti e la relativa descrizione.

Impatto (I)	Descrizione dell'impatto	Valore
Basso	Gli individui non saranno impattati dalla Violazione o potrebbero essere impattati da alcuni superflui inconvenienti, che saranno in grado di superare senza alcun problema.	1
Medio	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà.	2
Alto	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà.	3
Molto alto	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare.	4

Definiti Impatto (I) e Probabilità (P) e moltiplicando il valore assegnato tramite la formula “I x P” (impatto X probabilità), si otterrà, il livello di rischio associato ad ogni singola minaccia.

Rischi	Probabilità (P)	Impatto (I)	Livello di rischio associato (P x I)
Accesso illegittimo ai dati	1	3	3
Modifica non desiderata dei dati	1	1	1
Perdita dei dati	1	1	1

Il DPIA, quindi si conclude con la valutazione complessiva del rischio associato alle attività di trattamento individuate. La valutazione finale sul rischio si ottiene tenendo in considerazione il valore massimo tra quelli associati alle singole minacce.

Di seguito viene riportato l'intervallo tramite cui è possibile assegnare una classificazione sul livello di rischio ottenuto al termine del DPIA.

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

Quindi, con riferimento allo specifico trattamento oggetto della valutazione:

Rischi	Descrizione delle principali fonti di rischio	Descrizione degli impatti potenziali	Livello di rischio associato	Accettabile (A)/ Migliorabile (M)
Accesso illegittimo ai dati	Attacco Hacker esterno, difetto dei sistemi, errore umano, condotte dolose interne	Perdita di riservatezza su dati relativi alla salute connessi a patologia grave	3	A
Modifica non desiderata dei dati	difetto dei sistemi, errore umano, condotte dolose interne	Fallimento dello studio	1	A
Perdita dei dati	Attacco Hacker esterno, difetto dei sistemi, errore umano, condotte dolose interne	Fallimento dello studio	1	A

Descrizione del piano d'azione (ove necessario)

Misure aggiuntive richieste	Responsabile	Tempo di completamento
Nessuna		

Valutazioni conclusive

Opinione degli interessati o dei loro rappresentanti (ove raccolta)

Non richiesta

Parere del Responsabile Protezione Dati (DPO)

Esaminata la presente valutazione d'impatto, i rischi previsti e le misure di sicurezza applicate a riduzione degli stessi, si ritiene che il trattamento in questione possa risultare compatibile con la normativa vigente in materia di protezione dati personali. Resta riservata la possibilità di svolgere successive verifiche e anche di modificare il presente giudizio a seguito di eventuali incidenti, reclami degli interessati e/o segnalazioni delle Autorità competenti.

Validazione della DPIA

Sottoscrizioni	Firma	Data
Il Dirigente proponente	 ALESSANDRO SARTESCHI 14:09:2026 14:49:57 GMT+02:00	
Il Responsabile Protezioni dati		ANDREA CIARMIELLO 08.09.2026 14:37:44 GMT+02:00
Il Titolare del trattamento	 PATRIZIA MEO 03/09/2026 09:44:13 UTC+0200	

Aggiornamenti successivi:

Data	Aggiornamento
	

Signed with  NamirialSign