ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

DELIBERAZIONE DEL DIRETTORE GENERALE

(Nominato con D.P.G.R.T. n. 177 del 16/12/2016)

N° 137 del 07/05/2021

Oggetto: Valutazione d'impatto sulla protezione dei dati		
Struttura Proponente	Direzione Aziendale	
	S.S. Programmazione e Gestione Risorse Economiche	Cristina Gheri
	Responsabile del procedimento	Caterina Ferrari
	Estensore	Caterina Ferrari
Allegati n. 1		

IMMEDIATAMENTE ESEGUIBILE ☐

Conti Economici			
Spesa	**Descrizione Conto**	**Codice Conto**	**Anno Bilancio**

Eseguibile a norma di Legge dal 22/05/2021

Pubblicato a norma di Legge il 07 MAG. 2021

Inviato al Collegio Sindacale il 07 MAG. 2021

IL DIRETTORE GENERALE

di questo Istituto per lo studio, la prevenzione e la rete oncologica, con sede in Via Cosimo il Vecchio 2 - 50139 Firenze, in forza del D.P.G.R.T. n. 177 del 16/12/2016, prorogato con D.P.G.R.T. n. 172 del 18/12/2020 e con atto del Presidente della Giunta Regionale n. registrazione 0023084 del 20.01.2021

07 MAG. 2021

Visti:

- il Decreto Legislativo 30 dicembre 1992, n. 502 e successive modifiche ed integrazioni;
- la Legge Regionale Toscana 24 febbraio 2005, n. 40 di disciplina del Servizio Sanitario Regionale e successive modifiche ed integrazioni;
- la Legge Regionale Toscana 14 dicembre 2017, n. 74 che stabilisce che, a seguito dell'assorbimento delle funzioni dell'Istituto toscano tumori (ITT), l'Istituto per lo studio e la prevenzione oncologica assume la denominazione di Istituto per lo studio, la prevenzione e la rete oncologica (ISPRO);
- la Delibera GRT n. 490 del 7 maggio 2018 di parere favorevole sullo statuto e regolamento dell'ISPRO;
- la Delibera DG ISPRO n. 150 del 31 maggio 2018 di presa d'atto della Delibera GRT n. 490 del 7 maggio 2018 sopra menzionata;
- la Delibera DG ISPRO n. 11 del 13 gennaio 2020 con la quale è stato modificato/integrato il Regolamento di organizzazione e l'organigramma adottato con Delibera DG ISPRO n. 150 del 31 maggio 2018;
- il Regolamento (UE) del Parlamento europeo e del consiglio del 27 aprile 2016, "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)", di seguito GDPR;
- il Decreto Legislativo 196/2003 del 30 giugno 2003 e s.s. mm. "Codice in materia di dati personali".

Premesso che il GDPR all'art. 35 statuisce che «la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato».

Rilevata la necessità di tale valutazione in ragione del trattamento su larga scala di dati sensibili o di dati di natura estremamente personale o di categorie particolari di dati ex art 9 del GDPR.

Richiamata la Delibera DG ISPRO 25 giugno 2018 n. 175, con cui è stato individuato come Responsabile della Protezione del Dati (RPD) l'Avvocato Alessandro Mosti.

Dato atto che la presente valutazione d'impatto è stata validata dall'RPD, che nella sua valutazione ha evidenziato alcune aree di rischio su cui suggerisce di intervenire, invitando altresì la Direzione ad aggiornare e ampliare periodicamente il documento, nel rispetto del principio di miglioramento continuo.

Dato atto inoltre che la presente valutazione d'impatto è stata partecipata ai Direttori di S.C. e ai Responsabili di S.S.

Rilevata la legittimità e la congruenza dell'atto con le finalità istituzionali di questo Ente, stante l'istruttoria effettuata.

Con la sottoscrizione del Direttore Amministrativo f.f. e del Direttore Sanitario, ciascuno per quanto di competenza, ai sensi dell'art. 3 del Decreto Legislativo n. 502/1992 e ss.mm.ii..

DELIBERA

Per quanto esposto in narrativa che espressamente si richiama:

1. di approvare il documento di Valutazione d'impatto sulla protezione dei dati di cui all'allegato "A" (parte integrante e sostanziale del presente atto) ai fini dell'assolvimento degli obblighi previsti dall'art. 35 del GDPR;

2. di recepire e dare corso alle indicazioni dell'RDP contenute nel documento approvato;

3. di trasmettere il presente atto al Collegio Sindacale ai sensi dell'art. 42, comma 2, della L.R. Toscana n. 40/2005 contemporaneamente all'inoltro all'albo di pubblicità degli atti di questo Istituto.

IL DIRETTORE SANITARIO
(Dott. Riccardo Poli)

IL DIRETTORE AMMINISTRATIVO f.f.
(Dott. Mario Piccoli Mazzini)

IL DIRETTORE GENERALE
(Prof. Gianni Amunni)

STRUTTURE AZIENDALI DA PARTECIPARE:

TUTTE le Strutture di ISPRO

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

DOCUMENTO VALUTAZIONE DEI RISCHI

DATI ORGANIZZAZIONE

Generali

Organizzazione: Istituto per lo Studio, la Prevenzione e la Rete Oncologica
PIVA/CF: IT05872050488 / IT94158910482
Indirizzo: Via Cosimo II Vecchio n. 2 - 50139, Firenze - Italia
Tipo attività: Attività di servizi sanitari
Tel.: 055 32697821 | **Email:** segreteria.direzione@ispro.toscana.it | **PEC:** ispro@postacert.toscana.it

Legale rappresentante

Nome e cognome: Prof. Gianni Amunni
Email: direzione.generale@ispro.toscana.it

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

Premessa

Motivazione della valutazione

Il presente documento viene elaborato sulla scorta dell'articolo 35 del Regolamento UE 679/2016.
La valutazione d'impatto si rende necessaria alla luce di un'attenta autoanalisi compiuta in ragione del trattamento su larga scala di dati sensibili o di dati di natura estremamente personale o categorie particolari di dati, ex art. 9 del Regolamento UE 679/2016.

I.S.P.R.O. - Sintetica panoramica dell'Istituto

Sono attività di ISPRO:

- La valutazione e la sorveglianza epidemiologica relativa agli aspetti di stile di vita, le esposizioni ambientali e occupazionali e gli aspetti socio-economici collegati, la promozione e realizzazione di progetti di intervento nel campo della prevenzione in ambito oncologico, sia nella popolazione generale, sia in sottogruppi a rischio specifico.
- L'organizzazione, l'esecuzione ed il monitoraggio delle procedure diagnostiche correlate agli screening oncologici (mammografico, cervicale e colorettale), inclusi gli esami di laboratorio, promuovendo la centralizzazione delle stesse.
- La prevenzione terziaria, con specifico riferimento al controllo dopo terapia ed alla riabilitazione dei pazienti oncologici, anche attraverso modelli innovativi di sinergia con il volontariato.
- Le attività ambulatoriali, di laboratorio, diagnostiche e specialistiche.
- L'attività di informazione per il malato oncologico ed i suoi familiari sui servizi di diagnosi e cura e sulle strutture della rete oncologica regionale.
- Il supporto psicologico per il malato ed il nucleo familiare, in collaborazione con i servizi di psiconcologia delle aziende sanitarie e degli enti del servizio sanitario regionale, ed il numero verde gratuito 800 880101.
- La gestione del Registro Tumori della Toscana, del Registro di Mortalità Regionale, nonché delle Mappe di rischio oncogeno e del Centro operativo regionale (COR) per i tumori professionali.
- Il supporto scientifico, metodologico ed operativo per la programmazione, conduzione ed analisi delle sperimentazioni cliniche e degli studi osservazionali promossi nell'ambito della rete oncologica.
- La promozione, attuazione, diffusione e valorizzazione dell'attività di ricerca e di innovazione in ambito oncologico.
- L'attività di aggiornamento professionale, nell'ambito della prevenzione oncologica per le aziende e gli enti del servizio sanitario regionale e nazionale.
- Il coordinamento operativo e il supporto tecnico amministrativo della rete oncologica.
- L'esercizio delle funzioni di governo clinico in ambito oncologico con particolare riferimento alla definizione ed al monitoraggio delle raccomandazioni cliniche, dei percorsi diagnostici e terapeutici oncologici in raccordo con la direzione regionale competente e con l'Organismo toscano per il governo clinico.

ISPRO, inglobando le funzioni dell'ex Istituto Toscano Tumori, ha il coordinamento operativo della rete oncologica toscana, attraverso l'Organismo di Coordinamento della rete oncologica regionale. La rete oncologica della regione Toscana coordina tutte le attività di prevenzione, diagnosi, cura e ricerca in campo oncologico svolte nelle aziende sanitarie, negli altri enti del servizio sanitario toscano e nello stesso ISPRO.

In ISPRO è presente il Laboratorio Regionale di Prevenzione Oncologica, nato per rispondere alle esigenze di passaggio dal Pap test al test HPV come screening primario per il cancro della cervice uterina e dalla conseguente centralizzazione presso il Laboratorio di ISPRO di tutti gli esami HPV e Pap test di triage dei programmi di screening della Regione Toscana.

All'interno di ISPRO opera il CRL (Core Research Laboratory), le cui funzioni sono state assorbite dall' ex ITT. Il CRL ha il compito di svolgere ricerca di base sul cancro e in particolare sui meccanismi molecolari che sono alle sue origini, creando sinergie di sistema a livello di rete oncologica.

L'istituto promuove la più ampia concertazione e collaborazione con le Aziende Sanitarie ed Ospedaliero-Universitarie e con gli Istituti di Ricovero e Cura a Carattere Scientifico, al fine di perseguire obiettivi di coordinamento e di integrazione operativa nel settore della prevenzione oncologica.

L'Istituto, riconosciuto dalla Regione Toscana come Centro di Riferimento Regionale per la Prevenzione Oncologica – CRRPO, ha funzione di consulenza e supporto metodologico alle Aziende Sanitarie della Regione Toscana per l'attivazione dei programmi di screening. Il CRRPO svolge altresì funzioni di monitoraggio e verifica di qualità dei programmi di screening territoriali.

ISPRO è sede dell'Osservatorio Nazionale Screening – ONS, che è stato individuato dal Ministero della Salute come organo tecnico a supporto sia delle Regioni, per l'attivazione dei programmi di screening, che del Ministero stesso, per il monitoraggio e la valutazione di questi programmi. L'ONS è promotore inoltre di iniziative di formazione per gli operatori dello screening e supporta la produzione di materiale informativo, promuovendo anche una comunicazione di qualità. L'ONS

in collaborazione con le principali esperienze nazionali, si pone l'obiettivo primario di superare il divario esistente tra Centro-Nord e Sud.

In collaborazione con la Lega Italiana per la Lotta contro i Tumori – LILT Sezione di Firenze è presente, all'interno dell'Istituto, il "Centro di Riabilitazione Oncologica" (CeRiOn), attraverso il quale si è concretizzata un'importante sinergia tra servizio pubblico e associazione no profit, che offre, ai cittadini affetti da patologie oncologiche, trattamenti fisico-sanitari integrati con trattamenti psicologici e socio-sanitari, con l'obiettivo di prendersi cura della persona nella sua interezza (corpo e mente). Presso la sede di ISPRO di Villa delle Rose sono presenti oltre ai volontari della LILT sezione Firenze - Servizio Donna come prima, le seguenti associazioni: Toscana Donna, Associazione Stomizzati Toscani (ASToS), Associazione Italiana Prostatectomizzati (AIP), La Finestra.

L'Istituto, in conformità a quanto previsto dalla normativa vigente e dall'attuale Piano Sanitario e Sociale Integrato Regionale, ha istituito e regolamentato il Comitato di Partecipazione, la cui sede è presso il presidio ISPRO di Villa delle Rose, in via Cosimo il Vecchio 2 a Firenze.
Il Comitato tramite le associazioni di volontariato e di tutela rappresentate ed operanti attualmente presso l'Istituto, in accordo con l'URP Ufficio Relazioni con il Pubblico di ISPRO, affronta e discute temi quali:

- accoglienza dell'utenza;
- informazione ed educazione alla salute;
- umanizzazione delle cure;
- indagini di soddisfazione;
- miglioramento della qualità dei servizi;
- pubblica tutela.

Le Associazioni che hanno aderito al Comitato di Partecipazione sono:

- LILT sezione Firenze
- Toscana Donna
- La Finestra
- Cittadinanzattiva Toscana Onlus
- Federconsumatori
- Piccino Picciò
- Amici dell'ANT
- Associazione Stomizzati Toscani (ASTos)
- Associazione pubblica assistenza fratellanza popolare Peretola ODV Onlus

Definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 del Regolamento (UE) 2016/679).

Trattamento: qualsiasi operazione o insieme di operazioni, compiute, con o senza l'ausilio di processi automatizzati, e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4 del Regolamento (UE) 2016/679).

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4 del Regolamento (UE) 2016/679).

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4 del Regolamento (UE) 2016/679).

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento (art. 4 del Regolamento (UE) 2016/679).

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (art. 4 del Regolamento (UE) 2016/679).

Rischio: scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità (Linee-guida 17/EN WP248).

Gestione del rischio: l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio (Linee-guida 17/EN WP248).
«*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*»[1].
La valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità, contenendo:

- «*una descrizione dei trattamenti previsti e delle finalità del trattamento*»;
- «*una valutazione della necessità e proporzionalità dei trattamenti*»;
- «una valutazione dei rischi per i diritti e le libertà degli interessati";
- «le misure previste per:
  - «affrontare i rischi»;
  - «dimostrare la conformità al presente regolamento»

In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

- stabilendo il contesto: «*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio*";
- valutando i rischi: «*valutare la particolare probabilità e gravità del rischio*»;
- trattando i rischi: «*attenuando tale rischio*», «*assicurando la protezione dei dati personali*» e «*dimostrando la conformità al presente regolamento*».

Nota: la valutazione d'impatto sulla protezione dei dati svolta ai sensi del Regolamento generale sulla protezione dei dati è uno strumento per gestire i rischi per i diritti degli interessati, di conseguenza, adotta la loro prospettiva, come avviene in taluni settori (ad esempio, la sicurezza sociale). Al contrario, la gestione del rischio in altri settori (ad esempio in quello della sicurezza delle informazioni) è incentrata sull'organizzazione.

---

1 Cfr. considerando 84

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

Panoramica

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

S.C. screening e prevenzione secondaria		
	Stato valutazione	In lavorazione
IDENTIFICAZIONE	**Natura, ambito di applicazione, contesto e finalità del trattamento considerate**	**Si**, Il trattamento concerne la programmazione e l'esecuzione di interventi di screening oncologico relativo ai tumori della mammella, della cervice uterina e del colon-retto, in cui vi sono prove che l'effettuazione periodica degli esami di screening consente di modificare la storia naturale della malattia tumorale. Un esame di screening non è un esame diagnostico e conclusivo di per sé, ma ha lo scopo di selezionare, in una popolazione apparentemente sana, un piccolo numero di persone che ha un certo rischio di avere piccoli tumori o di alterazioni che potrebbero precedere un tumore. Queste persone saranno invitate a fare ulteriori accertamenti. Nello specifico, il trattamento ha ad oggetto la programmazione, l'organizzazione, la gestione, il monitoraggio e il controllo di qualità dell'attività di prevenzione secondaria per i tumori del cervico-carcinoma, del colon retto, della mammella. Queste attività sono svolte nel territorio della ex Azienda Sanitaria di Firenze, mentre il servizio di diagnosi precoce per le neoplasie cutanee e di follow-up dei melanomi opera all'interno della rete di servizi metropolitana. I dati raccolti mediante le attività di screening sono utilizzati, con il consenso dell'interessato e /o parere del Comitato Etico (CE) Locale, per attività di ricerca relativa alla prevenzione secondaria per i tumori della cervice uterina,del colonretto, della mammella e della cute in collaborazione con le strutture epidemiologiche presenti in ISPRO e gruppi di ricerca nazionali e internazionali. All'interno della struttura sono presenti due strutture semplici: SS Senologia di Screening e SS Centro di Riferimento Regionale per la Prevenzione Oncologica.
	Dati pers., destinatari e il periodo di conserv. registrati	**Si**, Nell'ambito del trattamento sono raccolti dati anagrafici, dati sanitari e dati genetici. I destinatari vengono individuati, sulla base di determinati parametri, tra la popolazione residente nel territorio della ex Azienda Sanitaria di Firenze, mentre il servizio di diagnosi precoce per le neoplasie cutanee e di follow-up dei melanomi opera all'interno della rete di servizi metropolitana. I dati personali sono conservati per un un periodo di tempo che tiene conto dell'offerta dell'intervento cioè almeno 30 anni per lo screening mammografico, 25 anni per lo screening per la ricerca del sangue occulto fecale, 40 anni per lo screening del collo dell'utero.
	Descrizione funzionale dei trattamenti fornita	**Si**, La coorte individuata sulla base di determinati parametri, viene inviata a partecipare agli esami di screening mediante raccolta di campione biologico presso i consultori dell'ex ASF. I campioni biologici vengono quindi consegnati presso il laboratorio di ISPRO, ove vengono analizzati. In caso di negatività, gli esiti sono comunicati al paziente mediante il servizio postale. In caso di positività, il referto torna alla U.O. competente, ove si valuta se procedere ad ulteriori approfondimenti diagnostici, ovvero alla fissazione di un nuovo controllo a 12 mesi.
	Risorse dei dati pers. individuate	**Si**, Il trattamento avviene mediante software e fogli di lavoro cartacei in uso presso ISPRO. Relativamente alla gestione informatizzata questa attività èsupportata da reti gestite da ESTAR nel rispetto dei più elevati standard di sicurezza. I campioni biologici raccolti nei luoghi individuati dal titolare sono trasferiti ad ISPRO mediante incaricati del titolare.
	Tenuto conto del rispetto dei codici di condotta approvati	**No**, Non vi sono codici di condotta concernenti le attività di screening.
NECESSITÀ	**Finalità determinate**	**Si**, Attività di screening oncologico e ricerca scientifica
	Finalità esplicite	**Si**, Le finalità sono esplicitate chiaramente nell'informativa
	Finalità legittime	**Si**
	Trattamenti leciti	**Si**, Nel contesto del trattamento in esame, la specifica base giuridica è costituita dall'art. 9, lettera h, del Regolamento Europeo n. 2016/679 (il trattamento è quindi lecito poiché effettuato per finalità di "diagnosi, assistenza o terapia sanitaria o sociale" quale quella di screening oggetto del percorso individuato). L'attività di ricerca scientifica viene svolta con il consenso dell'interessato e/o previo parere del CE Locale. **Motivi:** Consenso, Salvaguardia interessi vitali
	Dati pers. adeguati	**Si**
	Dati pers. limitati	**Si**
	Definiti limiti di conserv.	**Si**, I dati personali sono conservati per un un periodo di tempo che tiene conto dell'offerta dell'intervento cioè almeno 30 anni per lo screening mammografico, 25 anni per lo screening per la ricerca del sangue occulto fecale, 40 anni per lo screening del collo dell'utero
DIRITTI	**Interessati informati**	**Si**, Prima dell'inizio del trattamento, agli utenti è consegnata idonea informativa predisposta da di comune accordo da ASL Toscana Centro e ISPRO.
	Accesso garantito	**Si**, Il responsabile ha adottato procedure per l'esercizio dei diritti degli interessati.
	Portabilità garantita	**No**, Non è applicabile al trattamento in esame.
	Rettifica garantita	**Si**, Il responsabile ha adottato procedure per l'esercizio dei diritti degli interessati.
	Cancellazione garantita	**No**, Il trattamento rientra nei c.d. L.E.A.
	Opposizione garantita	**Si**, Il responsabile ha adottato procedure per l'esercizio dei diritti degli interessati.
	Limitazione garantita	**Si**, Il responsabile ha adottato procedure per l'esercizio dei diritti degli interessati.

	Gestiti rapporti con resp.	**Si**, Tutti i responsabili coinvolti nel trattamento sono stati nominati mediante articolato contratto.
	Consultazione preventiva	**No.**

ISPRO
istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

S.C. Senologia Clinica		
	Stato valutazione	In lavorazione
IDENTIFICAZIONE	**Natura, ambito di applicazione, contesto e finalità del trattamento considerate**	La Struttura Complessa di Senologia Clinica svolge le seguenti funzioni: - Provvedere alla gestione, organizzazione e controllo delle attività di diagnostica senologica clinica e strumentale in popolazione sintomatica o asintomatica auto selezionata. - Rappresentare il riferimento per la produzione di prestazioni diagnostiche, orientato alla standardizzazione dei processi ed alla appropriatezza degli interventi, garantendo un autonomo contributo alla gestione delle casistiche gestite in ambito clinico, in armonia con le strategie aziendali. - Assicurare agli utenti il pieno contributo nella soluzione dei problemi diagnostico-terapeutici mediante professionalità specifiche e risorse tecnologiche e strutturali, secondo criteri di appropriatezza e necessità. - Sviluppare la standardizzazione dei processi, contestualizzandoli alle condizioni cliniche del paziente. - Svolgere attività di controllo periodico clinico-strumentale per soggetti ad alto rischio eredo-familiare e con storia personale di carcinoma della mammella. - Partecipare, per quanto di competenza, all'attività di ricerca di ISPO e all'espletamento delle funzioni regionali di riferimento, didattica ed aggiornamento professionale. - Collaborare con le altre Aziende Sanitarie alla realizzazione di mammografie in pazienti asintomatiche non inserite nei percorsi di cui sopra. - Gestire progetti speciali (a fini di fattibilità e di ricerca), secondo i programmi definiti dalla struttura, anche con collaborazioni nazionali ed internazionali.
	Dati pers., destinatari e il periodo di conserv. registrati	**Si**, Vengono registrati i dati personali in formato digitale e/o cartaceo (dati anagrafici, sanitari, genetici. I dati personali sono conservati per un periodo di tempo che tiene conto dell'offerta dell'intervento cioè almeno 30 anni. I destinatari sono dipendenti ISPRO e dipendenti di altre Aziende Sanitarie (es. richieste di esami istologici).
	Descrizione funzionale dei trattamenti fornita	**Si.** Nella procedura di Struttura
	Risorse dei dati pers. individuate	**Si**, Il trattamento avviene mediante software in uso presso ISPRO, supportato da reti gestite da ESTAR nel rispetto degli standard di sicurezza.
	Tenuto conto del rispetto dei codici di condotta approvati	**No**, Non vi sono codici di condotta concernenti le attività di Senologia Clinica.
NECESSITÀ	**Finalità determinate**	**Si**, Le finalità sono esplicitate nel consenso informato sottoposto al paziente.
	Finalità esplicite	**Si**, Le finalità sono esplicitate chiaramente nell'informativa.
	Finalità legittime	**Si**
	Trattamenti leciti	**Si**, La base giuridica che legittima i trattamenti è l'interesse pubblico e, per quanto concerne le attività di ricerca scientifica, il consenso dell'interessato. **Motivi:** Consenso, Interesse pubblico
	Dati pers. adeguati	**Si.** Vengono raccolti i dati necessari e sufficienti all'erogazione dei trattamenti.
	Dati pers. limitati	**Si.** Vengono raccolti solo i dati necessari all'erogazione dei trattamenti.
	Definiti limiti di conserv.	**Si**, I dati personali sono conservati per un periodo di tempo di almeno 30 anni, che tiene conto della necessità di conoscere la storia clinica dei Pazienti e della necessità di confronto diagnostico con esami precedenti.
DIRITTI	**Interessati informati**	**Si.** L'informativa fornita all'interessato prevede la descrizione delle modalità di esercizio dei diritti
	Accesso garantito	**Si.** Il titolare ha adottato una procedura specifica per l'esercizio dei diritti.
	Portabilità garantita	**No**, Non è applicabile al trattamento in esame.
	Rettifica garantita	**Si**, Il titolare ha adottato una procedura specifica per l'esercizio dei diritti.
	Cancellazione garantita	**Si**, Il diritto di cancellazione è suscettibile di limitazione in ragione degli obblighi informativi cui è soggetto il Titolare.
	Opposizione garantita	**Si**, Il titolare ha adottato una procedura specifica per l'esercizio dei diritti.
	Limitazione garantita	**Si.** Il diritto alla limitazione è subordinato al rispetto degli obblighi informativi cui è soggetto il Titolare.
	Gestiti rapporti con resp.	**Si.** Tutti i i responsabili sono stati nominati con idoneo contratto, come previsto dal GDPR.

	Consultazione preventiva	**No.**

S.C. Attività tecnico amministrative		
	Stato valutazione	In lavorazione
	Dati pers., destinatari e il periodo di conserv. registrati	**Si**, Il periodo di conservazione dei dati è 10 anni. Trattasi di dati comuni e sensibili. A titolo esemplificativo: ragione sociale, cognome e nome, CF, recapiti di residenza/domicilio, recapiti mail, recapiti mail e telefonici, coordinate bancarie, dati reddituali e stato di salute.
	Descrizione funzionale dei trattamenti fornita	**Si**
	Risorse dei dati pers. individuate	**Si**, I dati condivisi sono custoditi sulla "rete aziendale K", mentre i dati su PC nel c.d. "spazio Z" riservato a ciascun incaricato. La documentazione cartacea è conservata in armadi custoditi presso ogni ufficio amministrativo.
	Tenuto conto del rispetto dei codici di condotta approvati	**No.**
NECESSITÀ	**Finalità determinate**	**Si**, Le finalità dei trattamenti sono preordinate al perseguimento di disposizioni di legge.
	Finalità esplicite	**Si**, Le finalità sono esplicitate nei protocolli aziendali.
	Finalità legittime	**Si**
	Trattamenti leciti	**Si** **Motivi:** Obbligo di legge
	Dati pers. adeguati	**Si**, I dati raccolti e trattati sono solo quelli strettamente indispensabili al perseguimento delle finalità di legge cui è preordinata l'azione della S.C.
	Dati pers. limitati	**Si**, I dati raccolti e trattati sono solo quelli strettamente indispensabili al perseguimento delle finalità di legge cui è preordinata l'azione della S.C.
	Definiti limiti di conserv.	**Si**, 10 anni
DIRITTI	**Interessati informati**	**Si**, Tutti i trattamenti sono eseguiti previa consegna di idonea informativa
	Accesso garantito	**Si**, Il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati. Il diritto di accesso è altreSì previsto nella Carta dei Servizi e Regolamento approvato con DDG 219/2017.
	Portabilità garantita	**Si**
	Rettifica garantita	**Si**, Il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati.
	Cancellazione garantita	**Si**, Il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati.
	Opposizione garantita	**Si**, Il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati.
	Limitazione garantita	**Si**, Il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati.
	Gestiti rapporti con resp.	**Si**, Tutti i responsabili esterni sono stati nominati con idoneo contratto.
	Consultazione preventiva	**No.**

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

S.C. Laboratorio regionale di prevenzione oncologica		
	Stato valutazione	In lavorazione
IDENTIFICAZIONE	**Natura, ambito di applicazione, contesto e finalità del trattamento considerate**	**Si**, Il Laboratorio Regionale di Prevenzione Oncologica (LRPO) è il laboratorio dedicato all'esecuzione di test di screening per la individuazione precoce dei tumori, all'esecuzione di test diagnostici e prognostici nell'ambito della prevenzione oncologica e alla ricerca applicata a nuovi test di screening, alla valutazione delle modalità di integrazione vaccino e screening, allo studio di fattori prognostici e di danno genotossico. Il Laboratorio nasce nel 2014 dalla fusione del Laboratorio di Citologia Analitica e Biomolecolare e del Laboratorio di Citopatologia. Questa integrazione si è resa necessaria per rispondere alle nuove esigenze di passaggio dal Pap test al test HPV come screening primario per il cancro della cervice uterina e dalla conseguente centralizzazione presso il Laboratorio di ISPRO di tutti gli esami HPV e Pap test dei programmi di screening della Regione Toscana. La progressiva implementazione del programma di screening HPV primario nell'intero territorio regionale attraverso il Laboratorio Regionale di Prevenzione Oncologica permette inoltre di evitare iniziative non coordinate con il progetto regionale stesso, nel rispetto del principio di appropriatezza e razionalizzazione dell'uso delle risorse. E' presente un settore dedicato alla ricerca del sangue occulto nelle feci, eseguita nell'ambito di programmi di screening per la prevenzione dei tumori colorettali. Biologi, Biotecnologi e Tecnici di laboratorio Biomedico svolgono nell'ambito delle proprie competenze e professionalità le attività svolte dalla struttura. Le attività principali della Struttura si concentrano su: Esecuzione dei test HPV di screening per tutti i programmi di screening della ex Azienda Sanitaria di Firenze e delle ex Aziende Sanitarie delle 3 aree vaste toscane, nonché di quelli eseguiti all'interno dei protocolli di sorveglianza post-trattamento e richiami precoci, gestione, preparazione e lettura dei Pap test di screening e dei Pap test di triage eseguiti all'interno dei programmi di screening della ex Azienda Sanitaria di Firenze e di altre ex Aziende Sanitarie delle 3 aree vaste toscane, nonché di quelli eseguiti all'interno dei protocolli di sorveglianza post-trattamento e richiami precoci. Gestione di esami citologici extravaginali: mammari, urinari e polmonari, nonché attività di citoassistenza. Processazione e refertazione esami per la ricerca del sangue occulto fecale per il programma della ex Azienda Sanitaria di Firenze. Attività di ricerca per l'analisi del danno genotossico e di altri aspetti di suscettibilità individuale ai tumori. Studi analitici su fattori di rischio oncogeno. Tipologia delle prestazioni erogate: L'attività del Laboratorio si esplica in un ambito multidisciplinare che comprende l'esecuzione di esami citologici, molecolari, biochimici ed immunocitochimici. Gli esami citologici sono eseguiti sia in un contesto di screening (Pap test) per la prevenzione del cancro della cervice, che di diagnosi precoce o di completamento diagnostico (citologia mammaria, urinaria, polmonare, organi profondi, linfonodi, liquidi pleurici, pericardici, ascitici, ecc.). La ricerca di sangue occulto nelle feci è eseguita nell'ambito di programmi di screening per la prevenzione dei tumori colorettali. Gli esami molecolari, come la ricerca di HPV ad alto rischio oncogeno, sono eseguiti all'interno di programmi di screening per la prevenzione del cancro della cervice sia come test primario o di triage, mentre la genotipizzazione HPV viene eseguita esclusivamente su richiesta medica. All'interno della Struttura Complessa sono presenti due Strutture Semplici: S.S. Citologia Extravaginale S.S. Diagnostica Molecolare Oncologica
	Dati pers., destinatari e il periodo di conserv. registrati	**Si**, Dati comuni: Cognome, nome, comune di nascita, provincia di nascita, stato di nascita, data di nascita, esenzioni, Codice Fiscale ed altri numeri di identificazione, Indirizzo E-Mail , Numero di telefono/cellulare,sesso m/f, domicilio, residenza. Dati relativi alla salute: Stato di salute, Patologie in atto, patologie pregresse, Pregressi trattamenti, Terapie in atto, Carta sanitaria, numero di gravidanze, Stato Gravidanza, Stato Menopausa, Contraccettivi usati, dati impianto protesi mammaria, tipologia di protesi. Destinatari: pazienti/Utenti Periodo di conservazione: I dati di esami in formato elettronico verranno conservati a tempo indeterminato. Il materiale cartaceo sarà conservato per il periodo di tempo necessario al conseguimento delle finalità della raccolta ovvero per il maggior periodo di tempo stabilito dalle normative di settore e dal prontuario di scarto di ambito sanitario. Decorsi tali termini di conservazione, i dati saranno distrutti o resi anonimi.
	Descrizione funzionale dei trattamenti fornita	**Si**, Nell'informativa privacy è indicata una descrizione del trattamento.
	Risorse dei dati pers. individuate	**Si**
	Tenuto conto del rispetto dei codici di condotta approvati	**No**, N.a.
NECESSITÀ	**Finalità determinate**	**Si**, Le finalità del trattamento sono indicate nel rispetto del vigente quadro normativo
	Finalità esplicite	**Si**
	Finalità legittime	**Si**, Le finalità sono coerenti con il quadro normativo di riferimento.
	Trattamenti leciti	**Si** **Motivi:** Consenso, Interesse pubblico
	Dati pers. adeguati	**Si**, I dati raccolti sono necessari e non eccedenti rispetto alle finalità del trattamento
	Dati pers. limitati	**Si**, I dati raccolti sono necessari e non eccedenti rispetto alle finalità del trattamento
	Definiti limiti di conserv.	**Si**, Dati di esami in formato elettronico verranno conservati a tempo indeterminato per le finalità di screening. Il materiale cartaceo sarà conservato per il periodo di tempo necessario al conseguimento delle finalità della raccolta ovvero per il maggior periodo di tempo stabilito dalle normative di settore e dal prontuario di scarto di

		ambito sanitario. Decorsi tali termini di conservazione, i dati saranno distrutti o resi anonimi.
DIRITTI	**Interessati informati**	**Si**, Il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati.
	Accesso garantito	**Si**, Il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati.
	Portabilità garantita	**No**, N.a.
	Rettifica garantita	**Si**, Il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati.
	Cancellazione garantita	**Si**, Il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati. Il diritto alla cancellazione potrebbe essere limitato nel rispetto della normativa dettata in materia di L.E.A.
	Opposizione garantita	**Si**, Il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati.
	Limitazione garantita	**Si**, Il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati. Il diritto alla limitazione potrebbe essere limitato nel rispetto della normativa dettata in materia di L.E.A.
	Gestiti rapporti con resp.	**Si**, Tutti i responsabili e i sub-responsabili sono stati adeguatamente nominati mediante apposito e specifico atto.
	Consultazione preventiva	**No.**

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

Valutazione per S.S. Centro di Riabilitazione Oncologica (Ce.Ri.On.)		
	Stato valutazione	In lavorazione
IDENTIFICAZIONE	**Natura, ambito di applicazione, contesto e finalità del trattamento considerate**	**Si**, Natura: documentazione cartaceo e digitale. Ambito: Dati comuni e sensibili - Dati relativi alla salute - Carte sanitarie- patologie attuali e pregresse, terapie in corso. Contesto: Utenti con esiti di patologie oncologiche. Associazioni di Volontariato. Finalità: Recupero psicofisico degli esiti conseguenti a patologie oncologiche. Collaborazione per attività socio-sanitarie.
	Dati pers., destinatari e il periodo di conserv. registrati	**Si**, Dati personali trattati: dati anagrafici, diagnosi e trattamento sanitario. Destinatari: medici di medicina generale, medici specialisti e su richiesta il paziente. Periodo di conservazione: 5 anni.
	Descrizione funzionale dei trattamenti fornita	**Si**
	Risorse dei dati pers. individuate	**Si**
	Tenuto conto del rispetto dei codici di condotta approvati	**No**, N.a.
NECESSITÀ	**Finalità determinate**	**Si**, Le finalità del trattamento dei dati personali sono per attività di prevenzione, cura e riabilatizione del paziente. Per l'erogazione di prestazioni ambulatoriali e di attività sanitarie di volontariato. In forma anonima per attività di studio, didattica e ricerca scientifica.
	Finalità esplicite	**Si**, Le finalità dei trattamenti sono chiarite nell'informativa.
	Finalità legittime	**Si**
	Trattamenti leciti	**Si** **Motivi:** Consenso, Salvaguardia interessi vitali
	Dati pers. adeguati	**Si**, Vengono raccolti solo i dati strettamente necessari all'erogazione dei trattamenti.
	Dati pers. limitati	**Si**, Vengono raccolti solo i dati strettamente necessari all'erogazione dei trattamenti.
	Definiti limiti di conserv.	**Si**, 5 anni
DIRITTI	**Interessati informati**	**Si**, Mediante idonea informativa.
	Accesso garantito	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Portabilità garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Rettifica garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Cancellazione garantita	-, -
	Opposizione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Limitazione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Gestiti rapporti con resp.	**Si**
	Consultazione preventiva	**No.**

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

Valutazione per Coordinamento di Area Infermieristica e URP		
	Stato valutazione	In lavorazione
IDENTIFICAZIONE	**Natura, ambito di applicazione, contesto e finalità del trattamento considerate**	**Si**, Natura: Il Coordinamento di Area Infermieristica ha al suo interno la gestione di: -personale afferente: Infermieri, Assistenti Sanitari, Dietista, Ostetriche, Operatori Socio Sanitari -Ufficio URP _Sorveglianza Sanitaria Documentazione cartaceo e digitale. Ambito: Dati comuni e sensibili - Dati relativi alla salute - Patologie attuali e pregresse, terapie in corso. Contesto: dipendenti di ISPRO e utenti che scrivono ad URP Finalità: La **sorveglianza sanitaria** è l'insieme degli atti medici svolti dal medico competente finalizzati alla tutela dello stato di salute e alla sicurezza dei lavoratori, in relazione all'ambiente di lavoro, ai fattori di rischio professionali e alle modalità di svolgimento dell'attività lavorativa. Finalità: **URP** necessari per lo svolgimento di funzioni istituzionali, per rispondere alle richieste degli utenti Dipende dal servizio alcuni dati sono conservati per un periodo illimitato altri per 10 anni. Il periodo di conservazione è descritto nel massimario di scarto.
	Dati pers., destinatari e il periodo di conserv. registrati	**Si**, Dati personali trattati: dati anagrafici, diagnosi e trattamento sanitario, cartelle sanitarie, reclami, richieste di risarcimento. Destinatari: dipendenti ISPRO, utenti URP
	Descrizione funzionale dei trattamenti fornita	**Si**
	Risorse dei dati pers. individuate	**Si**, I dati sono custoditi sulla "rete aziendale K", mentre i dati su PC nel c.d. "spazio Z" riservato a ciascun incaricato. La documentazione cartacea è conservata in armadi custoditi presso ogni ufficio preposto.
	Tenuto conto del rispetto dei codici di condotta approvati	**No**, N.a.
NECESSITÀ	**Finalità determinate**	**Si**, Le finalità dei trattamenti sono preordinate al perseguimento di disposizioni di legge.
	Finalità esplicite	**Si**, Le finalità dei trattamenti sono esplicitate nelle procedure aziendali e nella Carta dei Servizi.
	Finalità legittime	**Si**
	Trattamenti leciti	**Si** **Motivi:** Consenso, ed obbligo di legge.
	Dati pers. adeguati	**Si**, Vengono raccolti solo i dati strettamente necessari all'erogazione dei trattamenti.
	Dati pers. limitati	**Si**, Vengono raccolti solo i dati strettamente necessari all'erogazione dei trattamenti.
	Definiti limiti di conserv.	**Si**, dal massimario di scarto
DIRITTI	**Interessati informati**	**Si**, Mediante idonea informativa.
	Accesso garantito	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati. Per URP il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati. Il diritto di accesso è altreSi previsto nella Carta dei Servizi e Regolamento approvato con DDG 219/2017.
	Portabilità garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Rettifica garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Cancellazione garantita	-, -
	Opposizione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Limitazione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Gestiti rapporti con resp.	**Si**
	Consultazione preventiva	**No.**

ISPRO
istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

Coordinamento di Area Tecnico Sanitaria		
	Stato valutazione	In lavorazione
IDENTIFICAZIONE	**Natura, ambito di applicazione, contesto e finalità del trattamento considerate**	**Si**, Natura Il trattamento concerne la programmazione, l'esecuzione di interventi di screening oncologico relativo ai tumori della mammella, la processazione dei campioni biologici relativi allo screening oncologico dei tumori della cervice uterina e del colon-retto, processazione di campioni biologici relativi ad attività extrascreening ed il trattamento di riabilitazione dei pazienti oncologici Nello specifico, il trattamento ha ad oggetto la programmazione, l'organizzazione, l'esecuzione e il controllo di qualità dei processi di produzione. Il Coordinamento di Area Tecnico Sanitaria ha al suo interno la gestione professionale degli operatori Tecnici Sanitari quali TSRM, TSLB FSK afferenti rispettivamente alle Strutture Funzionali Senologia Clinica, Prevenzione Secondaria e Screening Oncologici, Laboiratorio Regionale di Prevenzione Oncologica, Centro di Riabilitazione Oncologica Documentazione cartaceo e digitale. Ambito: Dati comuni e sensibili - Dati relativi alla salute - Patologie attuali e pregresse, terapie in corso. Contesto: dipendenti di ISPRO , utenti dei programmi di screening e dei percorsi di riabilitazione oncologica Finalità: il trattamento ha ad oggetto la programmazione, l'organizzazione, l'esecuzione dei test di screening e dei trattamenti riabilitativi, nonché il controllo di qualità dei processi di produzione.
	Dati pers., destinatari e il periodo di conserv. registrati	**Si**, Nell'ambito del trattamento sono raccolti dati anagrafici, dati sanitari. I dati personali sono conservati per un un periodo di tempo congruo alla tipologia di intervento (almeno 30 anni per lo screening mammografico) e secondo quanto previsto dal massimale di scarto
	Descrizione funzionale dei trattamenti fornita	**Si** Nell'informativa privacy è indicata una descrizione del trattamento.
	Risorse dei dati pers. individuate	**Si** Il trattamento avviene mediante software in uso presso ISPRO, supportato da reti gestite da ESTAR nel rispetto dei più elevati standard di sicurezza.
	Tenuto conto del rispetto dei codici di condotta approvati	**No**, Non applicabile.
NECESSITÀ	**Finalità determinate**	**Si**, Le finalità dei trattamenti sono preordinate al perseguimento di disposizioni di legge.
	Finalità esplicite	**Si**, Le finalità dei trattamenti sono esplicitate nelle procedure aziendali e nella Carta dei Servizi e nelle informative consegnate agli utenti
	Finalità legittime	**Si**
	Trattamenti leciti	**Si Motivi:** Consenso, ed obbligo di legge.
	Dati pers. adeguati	**Si**, Vengono raccolti solo i dati strettamente necessari all'erogazione dei trattamenti.
	Dati pers. limitati	**Si**, Vengono raccolti solo i dati strettamente necessari all'erogazione dei trattamenti.
	Definiti limiti di conserv.	**Si**, dal massimario di scarto
DIRITTI	**Interessati informati**	**Si**, Mediante idonea informativa.
	Accesso garantito	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati. Per URP il titolare si è dotato di idonea procedura per l'esercizio dei diritti degli interessati. Il diritto di accesso è altresì previsto nella Carta dei Servizi e Regolamento approvato con DDG 219/2017.
	Portabilità garantita	**No** Non applicabile
	Rettifica garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Cancellazione garantita	**No**, parte dei trattamenti rientrano nei L.E.A
	Opposizione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Limitazione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Gestiti rapporti con resp.	**Si**

	Consultazione preventiva	**No.**

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

S. S. Epidemiologia molecolare e dei fattori di rischio		
	Stato valutazione	In lavorazione
IDENTIFICAZIONE	**Natura, ambito di applicazione, contesto e finalità del trattamento considerate**	La S.S. Epidemiologia molecolare e dei fattori di rischio si occupa essenzialmente di progetti di ricerca.
	Dati pers., destinatari e il periodo di conserv. registrati	I tipi di dati raccolti sono: a) dati da questionari su abitudini alimentari, stile vita, storia riproduttiva, patologie pregresse del soggetto e dei familiari, uso di farmaci, misure antropometriche e di composizione corporea b) campioni biologici conservati in banca biologica e risultati di analisi di laboratorio comprendenti dati genetici epigenetici c) dati di follow up dei soggetti riguardo ad eventi sanitari (diagnosi di tumore e altre patologie croniche). I dati in formato elettronico, trasmessi in forma anonima, verranno conservati a tempo indeterminato.
	Descrizione funzionale dei trattamenti fornita	**Si.** I dati raccolti con l'obiettivo di studiare il rapporto tra stile di vita, biomarcatori di rischio e il rischio di sviluppare un tumore o altra malattia cronica, vengono elaborati e presentati in maniera aggregata e sono oggetto di Report e pubblicazioni per la comunità scientifica. Vengono anche utilizzati per produrre materiali divulgativi per la popolazione e come base per Linee Guida. Il periodo di conservazione è legato alla durata dei progetti per i quali vengono raccolti /utilizzati e può essere non determinata per le coorti prospettiche sulle quali si inseriscono progetti di ricerca successivi. Questi aspetti sono tutti indicati nelle richieste di valutazione al CEL.
	Risorse dei dati pers. individuate	**Si**. Fonti informative sia su supporto cartaceo sia su supporto informatizzato. I documenti cartacei sono conservati in spazi ad hoc nella sede di lavoro (armadi chiusi a chiave dislocati in varie stanze o corridoi) e in parte in remoto. Inoltre, sono su supporti informatici ad accesso differenziato per gli autorizzati in relazione alla loro specifica attività nelle singole ricerche. Campioni biologici stoccati nella banca biologica della SC.
	Tenuto conto del rispetto dei codici di condotta approvati	**No**, N.a.
NECESSITÀ	**Finalità determinate**	**Si**, Le finalità sono indicate nei singoli protocolli di ricerca e sono quelle di studiare in generale il rapporto tra fattori ambientali, di stile di vita, legati alla storia personale e familiare di malattia e fattori genetici epigenetici il rischio di tumore e altre malattie croniche.
	Finalità esplicite	**Si**, le finalità dei trattamenti sono riportate nei singoli protocolli di ricerca
	Finalità legittime	**Si.**
	Trattamenti leciti	**Si** **Motivi:** Consenso per i progetti di ricerca e obbligo di legge per gli eventuali ulteriori trattamenti effettuati..
	Dati pers. adeguati	**Si**, Sono adeguati alle finalità dei singoli studi come specificati nei protocolli di ricerca approvati e finanziati.
	Dati pers. limitati	**Si**, Vengono raccolti solo i dati strettamente necessari all'erogazione dei trattamenti.
	Definiti limiti di conserv.	**Si**
DIRITTI	**Interessati informati**	**Si**, Mediante idonea informativa.
	Accesso garantito	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Portabilità garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Rettifica garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Cancellazione garantita	-, -
	Opposizione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Limitazione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Gestiti rapporti con resp.	**Si**
	Consultazione preventiva	**No.**

S. C. Epidemiologia clinica e supporto al governo clinico		
	Stato valutazione	
IDENTIFICAZIONE	**Natura, ambito di applicazione, contesto e finalità del trattamento considerate**	La SC svolge attività di valutazione degli screening oncologici oggetto dei Livelli Essenziali di Assistenza (LEA; screening per tumore alla mammella, cervice e colorettale; DPCM 29/11/2001). Sono inoltre condotti progetti di ricerca sia nell'ambito della valutazione di Health Technology Assessment (HTA) di nuove metodiche o politiche di screening nel campo dello screening per il tumore alla mammella, cervice e colorettale che riguardo alla diagnosi precoce del carcinoma del polmone e della prostata. È attribuita alla SC anche la ricerca in campo psico-oncologico e bioetico, in particolare su temi legati alla cura di malati inguaribili e alla innovazione in termini di comunicazione in quei setting. Vengono anche condotti specifici progetti di ricerca sul rapporto tra stile di vita, biomarcatori e rischio di tumore. Alla SC è affidata la gestione del Registro Tumori Regionale Toscano e delle attività di valutazione e ricerca a questo collegate.
	Dati pers., destinatari e il periodo di conserv. registrati	I tipi di dati raccolti sono: a) dati da questionari su stile vita in genere, storia riproduttiva, patologie pregresse del soggetto e dei familiari, uso di farmaci, esami di screening oncologici effettuati con eventuali approfondimenti, misure antropometriche, bisogni dei malati e dei curanti, qualità di vita e distress psicologico; b) campioni biologici conservati in banca biologica e risultati di analisi di laboratorio comprendenti dati genetici epigenetici; c) dati di follow up dei soggetti riguardo ad eventi sanitari (diagnosi di tumore e altre patologie croniche).
	Descrizione funzionale dei trattamenti fornita	Trattamenti nell'ambito di progetti di ricerca.
	Risorse dei dati pers. individuate	Fonti informative sia su supporto cartaceo sia su supporto informatizzato. I documenti cartacei sono conservati in spazi ad hoc nella sede di lavoro (armadi chiusi a chiave dislocati in varie stanze o corridoi) e in parte in remoto. Inoltre sono su supporti informatici ad accesso differenziato per gli autorizzati in relazione alla loro specifica attività nelle singole ricerche. Campioni biologici stoccati in banca biologica.
	Tenuto conto del rispetto dei codici di condotta approvati	**N.a.**
NECESSITÀ	**Finalità determinate**	**Si.** Le finalità sono indicate nei singoli protocolli di ricerca e sono quelle di studiare in generale il rapporto tra fattori ambientali, di stile di vita, legati alla storia personale e familiare di malattia e fattori genetici ed epigenetici, il rischio di tumore e altre malattie croniche. Inoltre, alla rilevazione dei bisogni di malati, familiari e curanti, di qualità di vita e di impatto di nuove modalità di comunicazione tra curanti, pazienti e loro familiari, in particolare in situazione di malattia inguaribile. Per quanto riguarda protocolli di ricerca per gli screening oncologici, le finalità sono legate all'individuazione dei migliori test di screening, all'intervallo di tempo più adeguato dopo il quale è utile effettuare un ulteriore esame di screening e all'individuazione delle migliori strategie organizzative al fine di aumentare la partecipazione della popolazione.
	Finalità esplicite	**Si.**
	Finalità legittime	**Si.** I trattamenti sono effettuati sulla base di un interesse pubblico nel settore della sanità pubblica.
	Trattamenti leciti	**Si.**
	Dati pers. adeguati	Sono adeguati alle finalità dei singoli studi come specificati nei protocolli di ricerca approvati e finanziati
	Dati pers. limitati	**No.**
	Definiti limiti di conserv.	**Si.** I dati in formato elettronico verranno resi anonimi e conservati a tempo indeterminato. Il materiale cartaceo sarà conservato per il periodo di tempo necessario al conseguimento delle finalità della raccolta. Decorsi i termini della conservazione, i dati saranno distrutti o resi anonimi.
DIRITTI	**Interessati informati**	**Si**, Mediante idonea informativa.
	Accesso garantito	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Portabilità garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Rettifica garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Cancellazione garantita	-, -
	Opposizione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Limitazione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Gestiti rapporti con resp.	**Si**

	Consultazione preventiva	**No.**

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

S.S. Registro Tumori		
	Stato valutazione	
IDENTIFICAZIONE	**Natura, ambito di applicazione, contesto e finalità del trattamento considerate**	I dati, sia anagrafici che relativi alla salute, sono trattati per la gestione del Registro Tumori Toscano , attività istituzionale di ISPRO, ex ISPO (Legge Regionale 3/2008), per finalità di rilevante interesse pubblico (Regolamento Regionale D.P.G.R. 64/R/2019) quali produzione misure di incidenza, mortalità, sopravvivenza e prevalenza dei tumori, conduzione di studi epidemiologici in ambito oncologico, anche in collaborazione con altri enti o strutture regionali, nazionali ed internazionali di ricerca scientifica, produzione di dati anonimi e aggregati per la programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, monitoraggio e valutazione dei dati relativi all'appropriatezza e qualità dei servizi diagnostici e terapeutici.
	Dati pers., destinatari e il periodo di conserv. registrati	I dati in formato elettronico trattati, sia anagrafici (nome, cognome, codice fiscale ed altri numeri di identificazione, comune, provincia e stato nascita, comune, provincia e stato residenza) che relativi alla salute (anamnestici, ricoveri, prestazioni ambulatoriali,interventi chirurgici, procedure diagnostiche e terapeutiche, esami clinici, referti citoistologici e biomolecolari, certificati di morte), sono tenuti nel registro tumori con l'ausilio di strumenti elettronici e trattati. mediante l'utilizzo di codici identificativi, conservati a tempo indeterminato. I dati cartacei sono conservati per il tempo necessario al conseguimento delle finalità della raccolta e poi distrutti.
	Descrizione funzionale dei trattamenti fornita	Implementazione e gestione del Registro Regionale Tumori
	Risorse dei dati pers. individuate	I dati raccolti si basano su fonti informative in gran parte informatizzate e, in misura minore , su supporto cartaceo. Le fonti informatizzate sono archiviate su supporto informatico con accesso riservato ai soli autorizzati e i documenti cartacei sono conservati in armadi chiusi a chiave, in stanze con accesso controllato tramite codice riservato al personale autorizzato.
	Tenuto conto del rispetto dei codici di condotta approvati	**N.a.**
NECESSITÀ	**Finalità determinate**	**Si.** Le finalità del trattamento dati da parte del Registro Tumori sono individuate dalla legge Regionale 3/2008 e dal Regolamento Regionale D.P.G.R. 64/R/ 2019.
	Finalità esplicite	**Si**, anche mediante il sito istituzionale dell'ente.
	Finalità legittime	**Si.** La Struttura in esame opera sulla base di una apposita e specifica legge regionale, e acquisisce la documentazione sulla scorta di specifiche convenzioni con le Aziende sanitarie toscane.
	Trattamenti leciti	**Si.** Obbligo di legge
	Dati pers. adeguati	**Si.** I dati sono adeguati al perseguimento delle finalità previste dal Regolamento Regionale D.P.G.R. 64/R/2019
	Dati pers. limitati	**No.**
	Definiti limiti di conserv.	**Si.** I dati informatizzati sono conservati a tempo indeterminato. I dati cartacei sono conservati per il tempo necessario al conseguimento della finalità della raccolta e poi distrutti.
DIRITTI	**Interessati informati**	**Si.** Mediante idonea informativa pubblicata sul sito internet dell'ente come previsto dal Regolamento Regionale D.P.G.R. 64/R/2019
	Accesso garantito	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Portabilità garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Rettifica garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Cancellazione garantita	-, -
	Opposizione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Limitazione garantita	**Si**, ISPRO si è dotata di procedure per l'esercizio dei diritti degli interessati.
	Gestiti rapporti con resp.	**Si.** È in preparazione convenzione con l'associazione nazionale AIRTUM, in qualità di responsabile esterno, per la trasmissione dei dati individuali anonimi alla Banca Dati
	Consultazione preventiva	**No.**

ISPRO
istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

Rischi

RISCHI	Accesso abusivo dall'esterno o dall'interno alla rete **aziendale**	**GENERALI**	
		Fonti di rischio	Dipendente incurante, Dipendente non formato, Utente esterno malintenzionato
		Impatti potenziali	Perdita dei dati, Perdita di fiducia da parte di utenti, Alterazione dei dati
		Minacce	Assenza di policy di dominio per il blocco dello schermo in caso di inattività dell'utente con ripristino protetto da password, Assenza di policy per la complessità delle password (lunghezza, validità, complessità), Assenza di policy sui dispositivi aziendali che si collegano dall'esterno (notebook o smartphone), Assenza di policy sui dispositivi mobili con accesso ai dati aziendali, Assenza di procedure automatiche di verifica dei software e delle licenze installate, Assenza di un piano di test dei backup, Assenza di un regolamento che definisce l'uso dei dispositivi aziendali esterni, Assenza di un regolamento interno per l'utilizzo degli asset aziendali, Assenza di una procedura di backup periodica automatica su supporti esterni rimovibili o su cloud, protetti da cifratura, Attacco informatico, Cattiva custodia delle chiavi, Perdita dei dati, Dipendente non formato, Mancanza di un regolamento interno per l'accesso e l'uso di internet e posta elettronica
		VALUTAZIONE DEL RISCHIO	
		Probabilità (P): 3	**Gravità (G):** 3 — **Rischio (P x G):** 9
		MISURE	
		Descrizione	Backup
		Attuazione	Adozione politiche di back-up nel rispetto dei più elevati standard disponibili.
		Addetti attuazione	Estar, Responsabile IT
		Attuata	Si
		Riduzione rischio	7 (Agisce direttamente sul valore del rischio)
		Asset	Intera struttura informatica di I.S.P.R.O.
		Descrizione	Archiviazione
		Attuazione	Provvedere all'archiviazione dei documenti cartacei e informatici nel rispetto delle procedure aziendali.
		Addetti attuazione	Incaricati al trattamento
		Attuata	Si
		Riduzione rischio	Mediamente (Agisce sulla probabilità del rischio)
		Asset	Intera struttura informatica di I.S.P.R.O.
		Descrizione	Attuazione norme di sicurezza
		Attuazione	Rispetto delle procedure aziendali dettate allo scopo di incrementare i livelli di sicurezza.
		Addetti attuazione	Incaricati
		Attuata	Si
		Riduzione rischio	Mediamente (Agisce sulla probabilità del rischio)
		Asset	Intera struttura informatica di I.S.P.R.O.
		Descrizione	Gestione del personale
		Attuazione	Pianificare e dare attuazione ad attività formativa rivolta a tutto il personale dedicata alla
		Addetti attuazione	Direzione amministrativa
		Attuata	Si
		Riduzione rischio	Mediamente (Agisce sulla probabilità del rischio)
		Asset	Intera struttura informatica di I.S.P.R.O.

		Descrizione	Gestione postazioni
		Attuazione	Adozione e implementazione di procedura relativa alla periodica manutenzione dell'hardware aziendale, alla sostituzione (e distruzione) di asset informatici vetusti, danneggiati o problematici e di aggiornamento periodici del software aziendale in uso.
		Addetti attuazione	Responsabile IT
		Attuata	Si
		Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
		Asset	Intera struttura informatica di I.S.P.R.O.
		Descrizione	Sicurezza della rete
		Attuazione	Le politiche di sicurezza informatica sono affidate ad ESTAR che vi provvede nel rispetto dei più elevati standard disponibili, anche mediante installazione e aggiornamento costante di firewall di tipo hardware o software, sistemi di monitoraggio anti-intrusione.
		Addetti attuazione	Estar, Responsabile IT
		Attuata	Si
		Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
		Asset	Intera struttura informatica di I.S.P.R.O.
RISCHI	Distruzione dei dati personali	**GENERALI**	
		Fonti di rischio	Dipendente incurante, Dipendente non formato
		Impatti potenziali	Alterazione della prestazione sanitaria in fase di diagnosi, prognosi e cura.
		Minacce	Assenza di un regolamento interno per l'utilizzo degli asset aziendali, Errore umano nella conservazione, Accessi ai sistemi non autorizzati da parte di esterni, Assenza di piani di formazione agli operatori relativi alle nuove tipologie di attacchi informatici (su social, via mail, via browser), Assenza di software di Data Loss Prevention, Assenza di un piano di test dei backup, Attacco informatico
		VALUTAZIONE DEL RISCHIO	
		Probabilità (P): 3	**Gravità (G):** 3 — **Rischio (P x G):** 9
		MISURE	
		Descrizione	Attuazione norme di sicurezza
		Attuazione	Rispetto delle procedure aziendali dettate allo scopo di incrementare i livelli di sicurezza.
		Addetti attuazione	Incaricati
		Attuata	Si
		Riduzione rischio	Mediamente (Agisce sulla probabilità del rischio)
		Asset	-
		Descrizione	Backup
		Attuazione	Adozione politiche di back-up nel rispetto dei più elevati standard disponibili.
		Addetti attuazione	Estar, Responsabile IT
		Attuata	Si
		Riduzione rischio	7 (Agisce direttamente sul valore del rischio)
		Asset	Intera struttura informatica di I.S.P.R.O.
		Descrizione	Archiviazione

		Attuazione	Provvedere all'archiviazione dei documenti cartacei e informatici nel rispetto delle procedure aziendali, riducendo al minimo l'utilizzo di dispositivi di archiviazione portatili (pen-drive, etc.).
		Addetti attuazione	Incaricati al trattamento
		Attuata	Si
		Riduzione rischio	Mediamente (Agisce sulla probabilità del rischio)
		Asset	-
		Descrizione	Gestione postazioni
		Attuazione	Adozione e implementazione di procedura relativa alla periodica manutenzione dell'hardware aziendale, alla sostituzione (e distruzione) di asset informatici vetusti, danneggiati o problematici e di aggiornamento periodici del software aziendale in uso.
		Addetti attuazione	Responsabile IT
		Attuata	Si
		Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
		Asset	Intera struttura informatica di I.S.P.R.O.
		Descrizione	Gestione del personale
		Attuazione	Pianificare e dare attuazione ad attività formativa rivolta a tutto il personale dedicata ai temi della privacy e della sicurezza.
		Addetti attuazione	Titolare
		Attuata	Si
		Riduzione rischio	Mediamente (Agisce sulla probabilità del rischio)
		Asset	-
RISCHI	**Divulgazione non autorizzata**	**GENERALI**	
		Fonti di rischio	Dipendente incurante, Terza parte malintenzionata
		Impatti potenziali	Perdita di fiducia da parte di utenti e autorità di controllo, Affetto psicologico a lungo termine o permanente
		Minacce	Software antivirus non dotato delle più recenti tecnologie (analisi comportamentale, ia), Assenza di piani di formazione agli operatori relativi alle nuove tipologie di attacchi informatici (su social, via mail, via browser), Attacco informatico, Errore umano nella conservazione
		VALUTAZIONE DEL RISCHIO	
		Probabilità (P): 3	**Gravità (G):** 3 — **Rischio (P x G):** 9
		MISURE	
		Descrizione	Lotta contro il malware
		Attuazione	Installazione e aggiornamento costante di firewall di tipo hardware o software, sistemi anti-intrusione, anti-virus e, occorrendo, DLP.
		Addetti attuazione	Estar, Responsabile IT
		Attuata	Si
		Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
		Asset	-
		Descrizione	Gestione del personale
		Attuazione	Pianificare e dare attuazione ad attività formativa rivolta a tutto il personale dedicata alla sicurezza dei dati e alle best practice in materia di conservazione e archiviazione

			dei dati, come previste nelle procedure aziendali.
		Addetti attuazione	Titolare
		Attuata	Si
		Riduzione rischio	Mediamente (Agisce sulla probabilità del rischio)
		Asset	-
RISCHI	**Modifica indesiderata dei dati personali**	**GENERALI**	
		Fonti di rischio	Dipendente incurante, Dipendente non formato, Terza parte malintenzionata
		Impatti potenziali	Alterazione della prestazione sanitaria in fase di diagnosi, prognosi e cura.
		Minacce	Attacco informatico
		VALUTAZIONE DEL RISCHIO	
		Probabilità (P): 3	**Gravità (G):** 3 — **Rischio (P x G):** 9
		MISURE	
		Descrizione	Backup
		Attuazione	Adozione politiche di back-up nel rispetto dei più elevati standard disponibili.
		Addetti attuazione	Estar, Responsabile IT
		Attuata	Si
		Riduzione rischio	7 (Agisce direttamente sul valore del rischio)
		Asset	-

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

Considerazioni preliminari sull'analisi dei rischi

A mente del Considerando 85 del GDPR «*una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione* d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla *reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata*».

Come previsto nel considerando 76, ISPRO adotta un sistema di calcolo del rischio basato su parametri oggettivi, al fine di stabilire se esiste un rischio o un rischio elevato per il trattamento specifico. L'oggettivazione del rischio pertanto passa attraverso un modello di creazione della probabilità e della gravità in grado di rispecchiare il contesto in cui l'organizzazione opera. Sono state identificate griglie oggettive di calcolo delle probabilità e gravità con riguardo ai diritti e alle libertà dell'interessato.

In esplicazione di quanto detto nel presente documento, sono riportati gli elementi previsti dalla normativa vigente (art. 35, comma 7):

1. La descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
2. La valutazione della necessità e proporzionalità dei trattamenti;
3. La valutazione dei rischi per i diritti e le libertà degli interessati;
4. Le misure previste per affrontare i rischi;

Le principali norme di riferimento in materia definiscono il rischio come "effetto dell'incertezza" (UNI EN ISO 9000) ovvero "effetto dell'incertezza sugli obiettivi" (UNI ISO 31000), dove l'effetto è uno scostamento da quanto atteso.
Il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento e della verosimiglianza del suo verificarsi, dove per verosimiglianza (o possibilità) s'intende la plausibilità di un accadimento ipotizzabile e, per conseguenze, s'intendono gli esiti di un evento che influenza gli obiettivi.
La verosimiglianza può essere descritta come probabilità (o frequenza, con riferimento ad un dato intervallo di tempo). Le conseguenze di un evento possono avere effetti positivi o negativi sugli obiettivi.
Pertanto, la definizione di rischio contenuta nelle Linee-guida 17/EN WP 248 è sovrapponibile con queste definizioni: "scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità".

Pertanto, il rischio può essere espresso come funzione di G (gravità delle conseguenze) e di P (probabilità di accadimento dell'evento), cioè:

$$R = G * P$$

ove:
R = entità del rischio
G = gravità delle conseguenze
P = probabilità di accadimento dell'evento

La procedura di valutazione dei rischi può essere riassunta come definito di seguito.
Ogni possibile minaccia viene analizzata sotto i seguenti profili:

- valutazione intrinseca della probabilità di accadimento dell'evento, in una scala da 1 a 4;
- valutazione della gravità delle conseguenze, in una scala da 1 a 4.

Per ogni possibile rischio identificato, come innanzi indicato, è effettuata la valutazione dell'entità del rischio.
La valutazione è corretta (ossia ricalcolata) in presenza di misure di prevenzione e opportunità identificate e adeguatamente attuate in relazione ai diversi aspetti esaminati. Si valuta così il rischio residuo, ossia il rischio che rimane a seguito del trattamento del rischio stesso.
Per valutare la Gravità, si tengono in considerazione il danno per la reputazione, la discriminazione, il furto d'identità, le perdite finanziarie, i danni fisici o psicologici, la perdita di controllo dei dati, altri svantaggi economici o sociali e, infine, l'impossibilità di esercitare diritti, servizi o opportunità.
Criteri di attribuzione dei livelli di Probabilità e Gravità.

R (entità del rischio)	**Probabilità**	Alta	4	Esiste una correlazione diretta tra la situazione rilevata ed il verificarsi dell'evento.

				Si sono già verificati eventi per la stessa situazione rilevata nel medesimo luogo, in ambienti simili o in situazioni simili. Il verificarsi dell'evento non susciterebbe alcuno stupore nell'organizzazione.
		Media	3	La situazione rilevata può provocare l'evento anche se non in modo automatico o diretto. È noto qualche episodio in cui si è verificato l'evento. Il verificarsi dell'evento susciterebbe una moderata sorpresa nell'organizzazione.
		Bassa	2	La situazione rilevata può provocare l'evento al contemporaneo verificarsi di particolari condizioni. Sono noti rari episodi già verificatisi. Il verificarsi dell'evento susciterebbe una discreta sorpresa nell'organizzazione.
		Non rilevante	1	La situazione rilevata può provocare l'evento per concomitanza di più eventi poco probabili indipendenti. Non sono noti episodi già verificatisi. Il verificarsi dell'evento susciterebbe incredulità.
	Gravità	Alta	4	Seria violazione della privacy di un interessato. Alto impatto su altri diritti fondamentali (es. diritto alla salute, libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione), con compromissione della fruizione. Conseguenze significative irreversibili o non eliminabili (minaccia per la vita, perdita o sospensione del rapporto di lavoro, danno finanziario ingente).
		Media	3	Violazione della privacy di un interessato con significativo disagio. Impatto su altri diritti fondamentali (es. diritto alla salute, libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione, incolumità della vita) che, in concomitanza con altri elementi, potrebbe comprometterne la fruizione. Conseguenze ripristinabili con un certo dispendio di risorse.
		Bassa	2	Violazione della privacy di un interessato con basso impatto (es. la violazione comporta un disturbo/disagio facilmente ripristinabile). Nessuna violazione di altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione).
		Non rilevante	1	Impatto irrilevante per la privacy di un interessato. Nessuna violazione di altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione).

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

Valutazione dei rischi per i diritti e le libertà dei soggetti

Classificazione dei rischi
Nella presente valutazione, i rischi sono classificati in base alle conseguenze e all'origine.

a) Conseguenze:
   - rischio di distruzione,
   - rischio di perdita,
   - rischio di modifica,
   - rischio di divulgazione non autorizzata,
   - rischio di accesso non consentito, a dati personali trasmessi, conservati o comunque trattati (art. 32, comma 2).

b) L'origine, la natura, la particolarità e la gravità dei rischi (cfr. Considerando 84). In particolare:
   - Vi sono rischi prospettabili come causati dal comportamento degli operatori/dipendenti difforme (per dolo o colpa).
   - Vi sono rischi prospettabili come causati dolosamente, ma anche fortuitamente, da eventi esterni che coinvolgono gli strumenti di lavoro e la struttura (sia informatici che materiali).
   - Vi sono rischi prospettabili come causati da eventi causali, ma prevedibili pur per astratto.

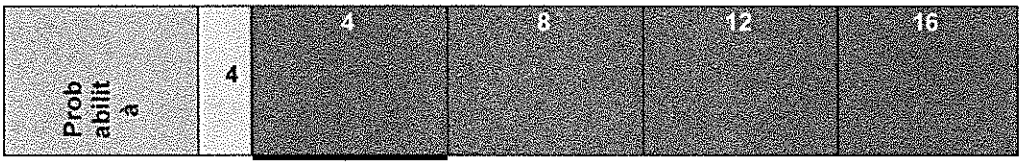
Gravità e tipologie di conseguenze
Sono stati, come evidenziato, individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati: in tale circostanza l'impatto potenziale consiste nella conoscenza di informazioni e dati personali trattati all'interno della struttura che possono causare un potenziale (da provare) rischio per la riservatezza dei soggetti interessati e nei casi di dati sensibili anche della dignità della persona, potenzialmente pregiudicata nel diritto a ricevere prestazioni sanitarie.

Per quanto concerne la probabilità del danno, atteso il settore in cui opera I.S.P.R.O. e la mole di dati trattati, si è stimata una probabilità di verificazione di un evento negativo compresa tra 2 e 3.
Parimenti, in relazione alla gravità, le conseguenze in caso di evento negativo sono state considerate particolarmente negative (tra 3 e 4), atteso che potrebbero comportare anche la discontinuità nell'erogazione di prestazioni sanitarie in persone affette da patologie gravi.
Prima dell'adozione delle misure di mitigazione, quindi, il rischio complessivo si attestava tra 9 e 12.
L'Istituto ha adottato una serie di misure di mitigazione che paiono idonee a gestire in maniera adeguata i rischi sottesi ai trattamenti svolti, in modo che

Rr < Ra

dove:
- **Ri (Rischio inerente)**: valore di riferimento su cui effettuare le valutazioni e le operazioni di mitigazione;
- **Ra (Rischio accettabile)**: il valore del rischio che il Titolare ritiene accettabile;
- **Rr (Rischio residuo)**: il valore del rischio successivamente agli interventi di mitigazione.

Il **Rischio inerente (Ri),** a seguito delle valutazioni svolte, è risultato superiore al **Rischio accettabile (Ra)**, e dunque il Titolare è intervenuto con misure di mitigazioni che paiono adeguate (e per la cui descrizione analitica si rimanda ai paragrafi che precedono).
Sebbene il **Rischio Residuo (Rr)** non possa essere completamente escluso, non di meno risulta contenuto in misura accettabile.
La quantificazione del **Rischio accettabile** è graficamente riportato nella tabella che segue:



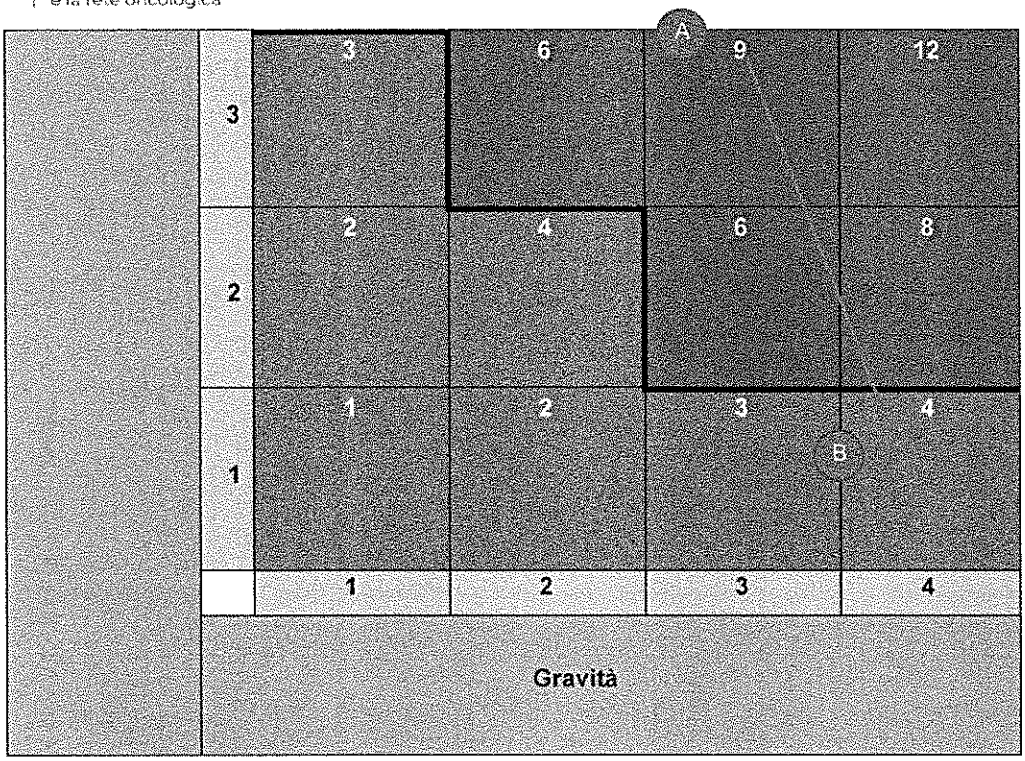
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		Gravità			

La matrice in tabella individua graficamente quelli che si considerano rischi non accettabili, ovvero quelli per cui è richiesto un intervento di miglioramento tale da riportare la situazione al di sotto della soglia di accettabilità. In base alla matrice dei rischi si individuano come non accettabili tutti quei rischi che risultano avere valori di P x G superiori a 4, unica eccezione le situazioni che si riferiscono ad un alto livello di probabilità (P = 4). Poiché non si considera accettabile alcun tipo di danno, neppure di lieve entità, qualora si ritenga il suo verificarsi estremamente probabile.

Le carenze eventualmente evidenziate sono oggetto di misure tecniche e organizzative e/o programmi di miglioramento definiti al fine di ridurre il rischio ad un livello accettabile, secondo il criterio di accettabilità enunciato.
Tali misure e programmi tengono conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento.

Nella tabella che segue si riporta, graficamente, le conseguenze delle misure di mitigazione adottate

Probabilità	4	4	8	12	16


A
B
3
6
9
12
2
4
6
8
1
2
3
4
1
2
3
4
Gravità

ISPRO
Istituto per lo studio, la prevenzione e la rete oncologica

Servizio Sanitario della Toscana

Valutazione del DPO

Nel complesso, il DPO rileva che la gestione dei rischi privacy connessi ai trattamenti svolti risulta essere adeguata:

- Il personale è adeguatamente organizzato, con una chiara definizione dei ruoli all'interno di ciascuna struttura;
- Estar cura la sicurezza informatica dell'Istituto nel rispetto di standard di sicurezza adeguati;
- Sono state adottate procedure chiare e precise relativamente all'utilizzo degli strumenti informatici, che prevedono una disciplina sulla complessità delle password e sulla frequenza delle modifiche, l'avvio del blocco dello schermo in caso di allontanamento dalla propria postazione, l'utilizzo della rete internet e delle mail e, in generale, su un utilizzo degli *asset* informatici consono alla scopo cui sono finalizzati.
- Le procedure di back-up sono adeguate quanto a frequenza e ridondanza;
- Sono fornite indicazioni precise in materia di archiviazione dei dati.

Occorre non di meno rilevare che, nel corso delle interviste effettuate ai dirigenti preposti a ciascuna struttura sono emerse alcune criticità, cui si suggerisce di porre rimedio tempestivamente. In particolare:

1. I dipendenti in *smart working* utilizzano *personal computer* propri e non aziendali, in assenza di indicazioni e procedure di sicurezza;
2. È stata segnalata una scarsa attenzione degli incaricati alle procedure di sicurezza da parte del Dott. Brancato (S.C. Senologia Clinica);
3. La S.C. Screening e prevenzione secondaria non è dotata di software che consenta l'invio di dati sanitari criptati a mezzo *e-mail*;
4. L'Istituto non risulta dotato di strumenti per la *Data Loss Prevention*, che parrebbe utile valutare;
5. Non è chiaro se vengano effettuati test di funzionamento dei *back-up*;
6. I dati cartacei sono spesso conservati in armadi non dotati di serrature;
7. Alcuni referenti (Dott. Palli) hanno evidenziato il rischio di contaminazione virus e malware e pericoli per browser di navigazione obsoleti: si suggerisce di verificare ed eventualmente procedere con i necessari aggiornamenti.
8. I referenti del Registro Tumori hanno segnalato i seguenti rischi: (a) Software antivirus non dotato delle più recenti tecnologie; (b) Assenza di piani di formazione agli operatori relativi alle nuove tipologie di attacchi informatici (su social, via mail, via browser); (c) Assenza di sistemi di controllo dell'accesso alle periferiche rimovibili (chiavette USB, unità DVD, lettori di memorie digitali, altro). Si suggerisce di adottare gli idonei correttivi.
9. La sicurezza informatica dell'Istituto è affidata a Estar, ente di supporto tecnico-amministrativo regionale, che garantisce elevati standard qualitativi nell'approntare le misure di sicurezza adeguate al rischio in essere. Non di meno, nonostante la richiesta, l'AdS di ISPRO non ha fornito una relazione chiara ed esaustiva in ordine alla sicurezza informatica dell'Ente.

In conclusione, sebbene l'attività di prevenzione dei rischi appaia soddisfacente, si invita l'Istituto a far fronte a tali aspetti.

Si consiglia una revisione del presente documento con cadenza almeno annuale.

Avv. Alessandro Mosti