REGOLAMENTO CONCERNENTE LA PROTEZIONE DEI DATI PERSONALI

INDICE

PARTE GENERALE

MODELLO ORGANIZZATIVO INTERNO: FIGURE DI RIFERIMENTO E COMPITI

TRATTAMENTO DEI DATI PERSONALI NEI RAPPORTI CON I TERZI

DIRITTI DEGLI INTERESSATI

SICUREZZA DEI DATI PERSONALI

MODALITÀ SPECIFICHE DI TRATTAMENTO DEI DATI PERSONALI

PARTE GENERALE

Art. 1 – Oggetto e ambito di applicazione

Il presente Regolamento disciplina le misure tecniche ed organizzative di protezione dei dati personali, nel rispetto di quanto previsto dal Decreto Legislativo n. 196 del 30.6.2003 e ss.mm.ii. e dal Regolamento UE 2016/679 del 27.4.2016 (di seguito anche "GDPR"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
Il presente Regolamento si applica a tutto il personale senza distinzione di ruolo e/o livello o di inquadramento. Pertanto tutti coloro che svolgono attività professionale, formativa o di volontariato presso lo IOV-IRCCS sono tenuti al rispetto di quanto prescritto nel presente Regolamento.

Art. 2 – Finalità e base giuridica del trattamento

1-L'Istituto Oncologico Veneto-IRCCS (di seguito IOV-IRCCS) è un Istituto di Ricovero e Cura a Carattere Scientifico di diritto pubblico, che persegue la prevenzione, la diagnosi e la cura delle patologie oncologiche.
Integrata all'attività assistenziale, è la ricerca scientifica in ambito oncologico perseguita secondo standard di eccellenza.
Lo IOV-IRCCS garantisce che il trattamento dei dati personali relativi alle persone fisiche si svolge nel rispetto dei diritti, delle libertà fondamentali e della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato.

2-Ai sensi dell'art. 5 del Regolamento (UE) 2016/679, lo IOV-IRCCS tratta dati personali e categorie particolari di dati in presenza delle condizioni di liceità previste dall'art. 6 e dall'art. 9 del Regolamento (UE)2016/679.
In particolare, la base giuridica del trattamento consiste:

- nell'esecuzione dei compiti di interesse pubblico e connessi all'esercizio di pubblici poteri attribuiti allo IOV-IRCCS da norme di legge o regolamento, ai sensi dell'art. 2-*sexies* del D. Lgs. 196/2003 e ss.mm.ii.;
- nell'adempimento di obblighi di legge cui è soggetto lo IOV-IRCCS;
- nella salvaguardia degli interessi vitali dell'interessato o altra persona fisica;
- nella necessarietà per finalità di diagnosi, assistenza o terapia sanitaria nonché di gestione dei sistemi e servizi sanitari;
- nella necessarietà per finalità di ricerca scientifica;
- nel consenso dell'interessato, laddove previsto.

3-Nel caso in cui il trattamento sia basato sul consenso, lo IOV-IRCCS provvede ad acquisire il consenso dell'interessato previa idonea informativa.

Art. 3 – Definizioni e termini: glossario privacy

Ai fini del presente Regolamento i termini e le espressioni di seguito indicati devono intendersi nel senso specificato.
Le definizioni che seguono costituiscono una terminologia comune in materia di protezione dei dati personali, pertanto i termini e le espressioni che seguono formano il "glossario privacy" e devono essere utilizzati in tutti i casi in cui sia necessario e nel significato di seguito specificato.
Nella stesura di documenti che richiedano l'uso di termini relativi alla protezione dei dati è fatto obbligo di consultare e utilizzare il glossario privacy.

TERMINE/ESPRESSIONE	TERMINI/ESPRESSIONI SIMILI	SIGNIFICATO
Archivio	***Banca di dati*** ***Database***	Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.
Autorità di Controllo	***Garante***	L'autorità pubblica indipendente istituita da uno Stato membro per verificare il rispetto della disciplina in materia di protezione dei dati personali: per l'Italia, tale autorità è il Garante per la protezione dei Dati Personali.
Autorizzato	***Incaricato***	La persona fisica autorizzata a compiere operazioni di trattamento dal Titolare e che agisce sotto la sua diretta autorità.
Comunicazione		Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione Europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione Europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione.
Consenso al trattamento dei dati personali	**Consenso privacy**	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso allo svolgimento di operazione di trattamento sui dati personali che lo riguardano.

Data breach		Si veda la definizione di "Violazione di sicurezza".
Diffusione		Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Dato/i Personale/i	**Dato/i identificativo/i**	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.
Dati ex art. 9 GDPR	**Dati Particolari** **Categorie particolari di dati** **Dati "sensibili"**	Ogni Dato Personale idoneo a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Dati ex art. 10 GDPR	**Dati Penali** **Dati Giudiziari**	Ogni Dato Personale relativo a condanne penali e ai reati o a connesse misure di sicurezza ovvero relativo a provvedimenti giudiziari, sanzioni penali, o carichi pendenti, o la qualità dell'imputato o indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale.
Dati anonimi		I dati che non si riferiscono a una persona identificata o identificabile; dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.

Dati biometrici		I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Data Protection Officer (DPO)	Responsabile della protezione dei dati (RPD)	È il soggetto designato dal Titolare del trattamento dei dati personali, selezionato tra persone che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto degli obblighi di legge. Ha un ruolo consultivo e di garanzia. Svolge mansioni relative all'implementazione dei sistemi di sicurezza e al rispetto degli adempimenti tecnici ed organizzativi prescritti, oltre al ruolo di principale referente per gli accertamenti e le richieste di informazioni provenienti dall'Autorità Garante
Delegato Privacy	Designato Privacy Delegato in materia di protezione dei dati personali	La persona fisica che, in virtù e nei limiti dei poteri di organizzazione, gestione e controllo conferiti dal Titolare del trattamento, è preposta all'esercizio delle funzioni di direzione, coordinamento e controllo delle attività di trattamento dei dati personali e dei correlati adempimenti previsti dal GDPR individuati nell'atto scritto di delega.
Destinatari		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.
Interessato		La persona fisica identificata o identificabile a cui si riferiscono i Dati Personali oggetto di trattamento.
Istanza		La richiesta che l'Interessato o un suo delegato o il tutore/ADS/curatore/esercente potestà genitoriale dell'interessato inoltra al Titolare del trattamento per esercitare i diritti riservati all'Interessato.

Limitazione di trattamento		Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.
Profilazione		Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
Pseudonimizzazione		Il trattamento cui sono sottoposti i dati personali affinché non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Regolamento UE 2016/679 in materia di protezione dei dati personali "General Data Protection Regulation"	**GDPR** **Regolamento**	Il Regolamento (UE) 2016/679 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).
Responsabile del trattamento	**Responsabile**	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Sub Responsabile del trattamento	**Sub Responsabile**	Qualsiasi soggetto, persona fisica o giuridica, a cui il Responsabile ricorra per l'esecuzione di specifiche attività di Trattamento per conto del Titolare a cui sono imposti gli stessi obblighi del Responsabile.

Terza Parte	**Terzo**	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare, il Responsabile e gli incaricati autorizzati al trattamento dei Dati Personali sotto l'autorità diretta del titolare o del responsabile.
Titolare del trattamento	**Titolare**	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, organizza e vigila sul processo di trattamento di dati personali e ne è responsabile. Ha potestà decisionale con riferimento ai fini, ai mezzi e alle modalità del trattamento ed è autonomo nel suo esercizio. L'Istituto Oncologico Veneto IRCCS, quale persona giuridica pubblica è il Titolare del trattamento dei dati.
Trattamento	**Operazione di 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.

Trattamento transfrontaliero		Trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro. È trattamento transfrontaliero il trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.
Violazione dei dati personali	***Violazione*** ***Data breach***	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Art. 4 – Principi generali del trattamento

Il trattamento dei dati personali è effettuato dallo IOV – IRCCS nel rispetto dei principi previsti dall'art. 5 del Regolamento (UE) 2016/679.

I dati personali oggetto di trattamento sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

b) sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità. Un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, del Regolamento UE, considerato incompatibile con le finalità iniziali;

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) esatti e, se necessario, aggiornati; vengono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

e) i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato;

f) i dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Art.5- Sistema interno di gestione della privacy

Lo IOV adotta, secondo il principio della responsabilizzazione *(accountability)*, le misure tecniche ed organizzative idonee a garantire che il trattamento dei dati sia effettuato nel pieno rispetto dei diritti e delle libertà degli interessati e in armonia con l'intera attività istituzionale.
Le misure organizzative adottate sono aggiornate periodicamente e nel loro insieme costituiscono il sistema interno di gestione della privacy, costituito da:

a) il Registro delle attività di trattamento dei dati;
b) il modello organizzativo in materia di protezione dei dati personali;
c) le autorizzazioni al trattamento dei dati nei gestionali informatici in uso presso lo IOV;
d) le informative sul trattamento dei dati agli interessati;
e) la valutazione preventiva dell'impatto privacy;
f) la prevenzione, il contenimento e la gestione delle violazioni dei dati personali;
g) la formazione dei delegati e degli autorizzati del trattamento dei dati.
h) Il sistema di gestione dei reclami e di gestione delle richieste relative all'esercizio dei diritti degli interessati;
i) le misure tecniche adottate per la protezione dei dati personali nel Dossier e nella cartella clinica elettronica.

Art. 6 – Rispetto dei codici deontologici

1-Lo IOV promuove il rispetto, da parte dei propri professionisti iscritti in albi professionali, delle disposizioni contenute nei rispettivi codici deontologici.

2-Qualunque trattamento di dati personali è effettuato in ottemperanza a quanto stabilito nei codici deontologici, pena la non liceità del trattamento stesso.

Art. 7– Politiche di accesso ai sistemi informativi aziendali e profili di autorizzazione

1-Nel rispetto del principio di minimizzazione del trattamento dei dati personali, la UOS Sistemi Informativi abilita il singolo utente ad accedere agli strumenti informatici e ai singoli applicativi informatici dello IOV – IRCCS compatibili con il ruolo professionale attribuito e con il centro di costo al singolo autorizzato e registrato nell'applicativo per la gestione delle risorse umane, su formale richiesta scritta del Direttore/Responsabile di Unità Operativa a cui l'utente stesso afferisce.

2-Periodicamente i Direttori/Responsabili di Unità Operativa, in qualità di Delegati Privacy aggiornano i profili di autorizzazione del personale assegnato quando ciò si renda necessario (a titolo esemplificativo, in caso di cessazione dal servizio, trasferimento ad altra Unità Operativa, cambiamenti di mansione).

3- Al fine di garantire che il trattamento dei dati inerenti allo stato di salute degli interessati sia effettuato con un idoneo livello di sicurezza, gli accessi ai software clinici e ai sistemi informativi aziendali sono tracciati.

Art.8 – Comunicazione di dati a terzi

Lo IOV effettua la comunicazione di dati personali a terzi, pubblici e privati, solo in conformità a quanto previsto dalle vigenti disposizioni legislative e regolamentari in materia, ricorrendo alle opportune misure di sicurezza, inclusa la pseudonimizzazione.

MODELLO ORGANIZZATIVO INTERNO: FIGURE DI RIFERIMENTO E COMPITI

Art. 9 – Il modello organizzativo aziendale in materia di privacy

In ottemperanza al principio di responsabilizzazione, lo IOV-IRCCS, **in qualità di Titolare**, individua i soggetti di riferimento in materia di dati personali.

Tenuto conto della struttura dello IOV-IRCCS descritta nell'Atto Aziendale, i soggetti di riferimento per la protezione dei dati personali sono:

- Il Titolare stesso;
- Responsabile della Protezione dei Dati (RPD o DPO);
- Il Delegato al trattamento di dati personali, o anche "Delegato Privacy";
- Gli Autorizzati al trattamento.

Ciascuna delle predette figure svolge i compiti in materia di protezione dei dati personali descritte negli articoli che seguono.

Trasversali all'articolazione sopra descritta sono:

- l'Ufficio Privacy
- la Unità Operativa Semplice Sistemi Informativi.

Art. 10– Titolare del trattamento dei dati

1-Il Titolare del trattamento dei dati personali è l'Istituto Oncologico Veneto-IRCCS nel suo complesso, rappresentato dal Direttore Generale. Al Titolare competono le decisioni in ordine ai fini, alle modalità e alla sicurezza del trattamento dei dati personali.

2-Il Titolare, avvalendosi del Responsabile della Protezione dei Dati (RPD), e con il supporto delle figure di volta in volta necessarie provvede a:

- Mettere in atto le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati sia effettuato conformemente ai principi del Regolamento (UE) 2016/679;
- Approvare il Modello Organizzativo aziendale in materia di protezione dei dati personali e alla revisione dello stesso, al fine di dare concreta attuazione al principio di *accountability;*
- Designare il Responsabile della Protezione dei Dati Personali e a comunicarne il nominativo e i dati di contatto all'Autorità Garante per la Protezione dei Dati Personali;
- Sottoscrivere gli accordi di nomina del Responsabile del trattamento, sia nel caso in cui un soggetto terzo debba trattare dati personali in nome e per conto dell'Istituto Oncologico Veneto–IRCCS, sia nell'ipotesi inversa, fatto salvo il caso in cui la sottoscrizione del contratto principale o altro negozio giuridico a cui è collegata la nomina a responsabile del trattamento sia stata delegata al Direttore/Responsabile di Unità Operativa funzionalmente competente;
- Sottoscrivere gli accordi di contitolarità e la documentazione a corredo degli stessi;
- Attribuire, mediante delega scritta, i compiti e le funzioni connessi alla protezione dei dati personali ai soggetti ("Delegati Privacy") che operano sotto la sua diretta autorità.

Art. 11– Responsabile della Protezione dei Dati

Lo IOV provvede alla designazione del Responsabile della Protezione dei Dati (RPD) in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa, delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti stabiliti per legge.

Il RPD dispone di risorse umane messe a disposizione dal Titolare per assolvere i suoi compiti.

Il Titolare del trattamento si assicura che il Responsabile della Protezione dei Dati agisca in piena autonomia e indipendenza nell'esecuzione dei compiti e non può essere delegato rispetto a compiti esecutivi.

Al Responsabile della Protezione dei Dati sono affidate le seguenti funzioni:

- **Svolge una funzione di sorveglianza e garanzia**: sorveglia l'osservanza del Regolamento

(UE) 2016/679, di altre disposizioni relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo. Nello svolgimento di tale funzione, il Responsabile Protezione Dati può rivolgersi a ciascuno dei soggetti di riferimento (i.e. Delegati, Autorizzati);

- Ha il compito di **sovraintendere a tutti i processi che riguardano il trattamento dei dati personali compiuti all'interno dell'Ente,** intervenendo in piena autonomia e indipendenza qualora individui problemi che potrebbero comportare un trattamento dei dati che presenti rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta;
- Svolge una **funzione consultiva**: il RPD informa e fornisce consulenza al Titolare del trattamento, ai delegati nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento (UE) 2016/679 nonché da altre disposizioni relative alla protezione dei dati;
- **Funzione di contatto**: il RPD coopera e funge da punto di contatto per il Garante per la privacy per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Gli interessati possono contattare il Responsabile della Protezione dei Dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti. A tal fine i dati di contatto del RPD sono pubblicati sul sito istituzionale: https://www.ioveneto.it/privacy/

Il RPD provvede a:

a) fornire supporto per l'adempimento di singoli obblighi previsti dal Regolamento quali: le informative (artt. 12-14); le designazioni dei responsabili del trattamento (art. 28) e delle persone autorizzate (art. 29), con suggerimenti circa le possibili istruzioni da impartire; il registro dei trattamenti (art. 30); il registro delle violazioni (art. 33);
b) rendicontare periodicamente l'attività svolta, sia quella in loco (mediante, ad esempio, la stesura di verbali degli incontri), sia quella a distanza, sullo stato del trattamento e della protezione dei dati personali;
c) partecipare alle attività di valutazione del rischio relativo alla sicurezza delle informazioni;
d) assistere il titolare nell'approvazione delle misure da adottare per la gestione dei rischi relativi alla protezione dei dati personali;
e) fornire attività di formazione e aggiornamento rivolte alle persone autorizzate al trattamento dei dati dall'ente.

Art. 12 – Ufficio privacy

L'Ufficio Privacy svolge i seguenti compiti:

a) aggiorna il Registro delle attività di trattamento sulla base delle informazioni fornite dai Delegati e dagli Uffici in staff con riferimento alle attività che comportano trattamento dei dati personali effettuate all'interno della propria UU.OO. e verifica l'aggiornamento del Registro da parte della UOS Sistemi Informativi per quanto attiene alle misure di sicurezza tecniche;
b) Predispone i modelli documentali ivi comprese le informative, le istruzioni operative per la relativa applicazione e le procedure necessarie per l'osservanza della disciplina in materia di protezione dei dati personali;
c) Fornisce il materiale di cui al punto precedente a ciascun Delegato Privacy;
d) Fornisce supporto a ciascun Delegato Privacy per quanto attiene agli adempimenti derivanti dalla normativa in materia di riservatezza e protezione dei dati personali;
e) Funge da punto di riferimento per il RPD;
f) Relaziona periodicamente l'attività svolta al Titolare e segnala i casi in cui i Delegati non forniscano le informazioni necessarie alla gestione del Registro dei trattamenti;
g) Supporta il Titolare nello svolgimento della valutazione d'impatto sulla protezione dei dati personali, secondo quanto previsto dall'art. 34 del presente Regolamento.

Art. 13- UOS Sistemi Informativi

La UOS Sistemi Informativi adotta le misure di sicurezza tecniche adeguate ad assicurare l'integrità e la disponibilità dei dati, dirette a garantire la protezione dei dispositivi e dei programmi contro il rischio di intrusione o perdita e il tempestivo ripristino dei dati personali in caso di incidente.
Inoltre, la UOS Sistemi informativi collabora con l'Ufficio Privacy ed il Responsabile della Protezione dei Dati nello svolgimento dei seguenti compiti:

- predispone misure di minimizzazione e, ove necessario, di pseudonimizzazione in caso di trattamento di dati particolari;
- predispone e aggiorna il Registro delle attività di trattamento per la parte relativa alle misure di sicurezza logiche e tecniche riferite all'infrastruttura e alle risorse informatiche aziendali;
- coopera, per i trattamenti a più alto rischio, nell'analisi dei rischi e nella predisposizione della valutazione di impatto privacy.

Tra le funzioni proprie del Servizio Sistemi Informativi connesse al corretto trattamento dei dati personali, rientra anche la vigilanza sul rispetto del Regolamento interno sull'utilizzo degli strumenti informatici e la verifica della coerenza delle richieste di abilitazione agli applicativi con i profili professionali ricavati dal sistema di gestione delle risorse umane e con i centri di costo cui appartengono gli utenti.

All'interno della UOS Sistemi Informativi vengono attribuite le funzioni di Amministratore di Sistema in conformità al Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali del 27 Novembre 2008 recante misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

Art. 14 – Delegato al trattamento dei dati

1-In considerazione della complessità e della molteplicità delle proprie funzioni istituzionali e della necessità di garantire a tutti i livelli l'osservanza della vigente normativa in materia di privacy, lo IOV– IRCCS, con il presente Regolamento, individua quali Delegati del trattamento, in relazione alle funzioni di specifica competenza derivanti dal rapporto giuridico esistente con l'Istituto stesso, i seguenti soggetti:

- Direttore Scientifico, Direttore sanitario e il Direttore Amministrativo;
- Direttori di Unità Operativa Complessa (U.O.C.);
- Direttori di Unità Operativa Semplice Dipartimentale (U.O.S.D.);
- Responsabili di Unità Operativa Semplice (U.O.S.) che non sia articolazione di Unità Operativa Complessa;
- Responsabili degli uffici/servizi in staff ai Direttori della Direzione Strategica;
- Sperimentatori principali o responsabili di studi clinici o osservazionali.

La funzione di Delegato del trattamento non è a sua volta delegabile. In caso di assenza o impedimento del Delegato del trattamento, le relative attribuzioni sono esercitate da chi lo sostituisce per le attività istituzionali.

2- In particolare il Delegato del trattamento deve:

a) trattare i dati personali osservando le disposizioni di legge e regolamentari, nonché le specifiche istruzioni impartite dal Titolare;
b) autorizzare, in nome e per conto del Titolare, i soggetti dell'ambito del proprio assetto organizzativo di competenza a svolgere le operazioni di trattamento di dati personali strettamente necessarie alle attività e alle funzioni assegnate, compresa l'eventuale assegnazione di profili informatici correlati alle proprie mansioni. Il Delegato richiede alla UOS Sistemi Informativi che gli autorizzati vengano abilitati agli applicativi necessari allo svolgimento delle mansioni lavorative, avendo cura che le stesse siano coerenti con il ruolo professionale ricoperto e con l'Unità Operativa/Ufficio di assegnazione;

c) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso la propria struttura, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;
d) rispettare e adottare tutte le misure tecniche ed organizzative predisposte dal Titolare;
e) mettere a disposizione del Titolare e del RPD e in caso di ispezioni tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa vigente;
f) verificare che la documentazione cartacea e digitale e le relative procedure informatizzate che supportano l'attività di trattamento dei dati di propria competenza, nonché i profili di autorizzazione degli incaricati al trattamento dei dati rispondano ai principi di necessità, pertinenza e non eccedenza;
g) verificare che all'interessato o al soggetto presso il quale sono raccolti i dati sia data l'informativa;
h) verificare che l'interessato o altro soggetto legittimato presti, quando previsto, il consenso al trattamento dei dati;
i) ottemperare ad ogni altro adempimento stabilito dal Titolare in relazione al trattamento dei dati personali;
j) collaborare con l'Ufficio Privacy e con la UOS Sistemi Informativi nell'espletamento dei rispettivi compiti; in particolare il Delegato deve:
    - fornire tutte le informazioni relative ai trattamenti di dati personali svolti all'interno della propria Unità Operativa necessarie alla gestione e all'aggiornamento del Registro delle attività di trattamento ed ogni altra informazione richiesta per l'attuazione degli obblighi normativi;
    - comunicare tempestivamente l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante ai fini della tutela della sicurezza e riservatezza dei dati personali, ivi compresa l'acquisizione di nuove risorse informatiche;
    - collaborare con il Titolare e con i soggetti sia interni sia esterni da questo incaricati nello svolgimento della valutazione d'impatto;
    - segnalare immediatamente all'Ufficio Privacy e in ogni caso entro e non oltre le 24 ore dalla scoperta i casi in cui a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi come incendi o altre calamità, si dovessero verificare la perdita, la distruzione o la diffusione indebita di dati personali trattati, secondo quanto previsto dalla normativa vigente in materia di protezione dei dati personali e dalla procedura per la gestione degli eventi potenzialmente qualificabili come *data breach* reperibile nell'Intranet aziendale.

3-I Delegati del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto previsto dalla vigente normativa in materia di privacy, dal presente Regolamento e dalle istruzioni ricevute nell'atto di delega, ivi comprese quelle riguardanti il Registro delle attività di trattamento, il rispetto delle misure di sicurezza e la ritardata o mancata attivazione degli adempimenti previsti dalla procedura per la gestione degli eventi potenzialmente qualificabili come *data breach* reperibile nell'Intranet aziendale.

4-L'Unità Operativa Complessa Gestione delle Risorse Umane, all'atto di conferimento di un nuovo incarico di Direttore di Unità Operativa Complessa, di Responsabile di Unità Operativa Semplice Dipartimentale e Unità Operativa Semplice provvede a:

a) integrare il contratto di lavoro mediante l'inserimento di un'apposita clausola che specifichi l'individuazione del soggetto quale Delegato del trattamento dei dati in relazione alle funzioni di competenza derivanti dall'incarico
b) comunicare al Servizio Sistemi Informativi ogni cessazione o altra variazione del predetto rapporto giuridico, che incida sulla figura di Delegato, per il blocco delle specifiche autorizzazioni precedentemente rilasciate per il trattamento dei dati.

5-Per coloro che alla data di entrata in vigore del presente Regolamento ricoprono già una delle funzioni indicate dal comma 1 del presente articolo, l'individuazione quale Delegato del

trattamento dei dati s'intende formalizzata e regolarizzata ad ogni conseguente effetto di legge con apposita delega scritta.
Per gli Sperimentatori principali o responsabili di studi clinici o osservazionali si rinvia all'art. 41 del presente regolamento.

Art. 15– Autorizzato al trattamento dei dati

1-Lo IOV – IRCCS, quale Titolare del trattamento, autorizza al trattamento dei dati personali le persone fisiche che operano sotto la sua diretta autorità.
2-In considerazione della complessità e della molteplicità delle proprie funzioni istituzionali e della necessità di garantire a tutti i livelli l'osservanza della vigente normativa in materia di privacy, l'Istituto Oncologico Veneto – IRCCS con il presente Regolamento individua quale Autorizzato del trattamento tutto il personale, anche convenzionato, che abbia con la stessa un rapporto giuridico di lavoro, di collaborazione, di consulenza, di prestazione d'opera professionale o di altra tipologia per lo svolgimento di attività, in relazione alle funzioni di specifica competenza derivanti dai rapporti giuridici instaurati.
Per coloro che alla data di entrata in vigore del presente Regolamento risultano avere già in atto un rapporto giuridico con lo IOV – IRCCS, l'individuazione quale Autorizzato al trattamento dei dati s'intende formalizzata e regolarizzata ad ogni conseguente effetto di legge con l'assegnazione in apposita struttura/ufficio.
3-Gli Autorizzati hanno accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti istituzionali di propria competenza, tramite l'assegnazione di profili informatici pertinenti e strettamente necessari per lo svolgimento delle attività e delle funzioni assegnate.
L'autorizzato ha il compito di trattare i dati in modo lecito, corretto, mantenendo la massima riservatezza; inoltre, deve trattare solo i dati necessari per lo svolgimento della propria attività, non deve divulgare i dati a soggetti non autorizzati, non deve effettuare un trattamento non autorizzato, deve verificare costantemente i dati personali, il loro aggiornamento, completezza e pertinenza.
Durante il trattamento o in caso di allontanamento dal posto di lavoro, l'Autorizzato si attiene alle istruzioni impartite dal Titolare e adotta le misure previste e a propria disposizione, secondo le istruzioni ricevute dallo IOV– IRCCS e dal Delegato privacy, per garantire che il trattamento di dati personali avvenga nel rispetto delle norme in materia e dei regolamenti e delle procedure interne.
Anche gli Autorizzati al trattamento che non sono tenuti per legge al segreto professionale, sono sottoposti a regole di condotta analoghe al segreto professionale e all'assunzione di comportamenti metodologicamente corretti in materia di riservatezza e di protezione dei dati.
4-La struttura competente alla gestione delle risorse umane all'atto di assunzione a qualsiasi titolo di personale o di conferimento di incarico professionale o di borsa di studio provvede a:

- predisporre il contratto di lavoro o di incarico o di borsa di studio mediante l'inserimento di un'apposita clausola che specifichi l'individuazione del soggetto quale Autorizzato del trattamento dei dati in relazione alle funzioni di competenza derivanti dal rapporto giuridico di cui al contratto con lo IOV-IRCCS;
- consegnare l'informativa sul trattamento dei dati personali e le istruzioni per le persone autorizzate al trattamento dei dati personali;
- acquisire la lettera di autorizzazione al trattamento dei dati personali, munita di sottoscrizione da parte del Delegato privacy e da parte dell'autorizzato per ricevuta e presa visione anche delle istruzioni di cui al punto che precede; per il personale sanitario del comparto e del ruolo tecnico di supporto (OSS) l'autorizzazione al trattamento dei dati personali viene sottoscritta in nome e per conto del Titolare del trattamento dal responsabile della funzione organizzativa della struttura sanitaria a cui afferisce;

- inserire e conservare l'autorizzazione al trattamento dei dati nel fascicolo personale del dipendente o convenzionato o nel fascicolo del professionista incaricato o nel fascicolo del beneficiario della borsa di studio;
- comunicare alla UOS Sistemi Informativi ogni spostamento interno, cessazione o altra variazione del predetto rapporto giuridico, che incida sulla figura di incaricato, per il blocco delle specifiche autorizzazioni precedentemente rilasciate per il trattamento dei dati.

5- Al tutor interno è affidato il compito di autorizzare, in nome e per conto del Titolare, il tirocinante al trattamento dei dati personali strettamente necessario per adempiere al progetto formativo relativo al tirocinio. La struttura competente alla gestione dei tirocini provvede al momento dell'avvio del tirocinio a consegnare l'informativa al tirocinante e a verificare unitamente al tutor interno i presupposti per il conferimento dell'autorizzazione al trattamento dei dati e a consegnare le istruzioni al trattamento al tirocinante autorizzato dal tutor interno.
La lettera di autorizzazione sottoscritta dall'autorizzato e dal tutor viene conservata dalla struttura competente alla gestione dei tirocini.

6- I frequentatori dell'Istituto, di regola, non sono tenuti a svolgere trattamento di dati personali del Titolare e non hanno accesso agli applicativi aziendali e a cura del direttore/responsabile della struttura frequentata sono edotti del rispetto delle regole di riservatezza.
7- I volontari dell'associazioni di volontariato che per convenzione prestano la loro attività di volontariato presso l'Istituto non sono tenuti svolgere trattamento di dati personali del Titolare e non hanno accesso agli applicativi aziendali. L'associazione ha l'onere di fornire formazione ai volontari sul rispetto della riservatezza e il direttore/responsabile della struttura frequentata dai volontari vigila sul rispetto delle regole di riservatezza.
8- Il Direttore/Responsabile della Unità Operativa sanitaria presso cui si svolge la formazione specialistica autorizza, in nome e per conto del Titolare, i medici specializzandi e gli specializzandi di area sanitaria (non medici) al trattamento dei dati personali per consentire lo svolgimento dell'attività formativa secondo le indicazioni della Scuola di specializzazione.
Il Direttore/Responsabile della Unità Operativa sede della formazione specialistica consegna le istruzioni per il trattamento dei dati personali allo specializzando e richiede l'accesso agli applicativi aziendali, limitatamente a quanto necessario allo svolgimento delle attività cliniche ed assistenziali previste dai percorsi formativi, alla UOS Sistemi Informativi – Servizio Abilitazioni.
Al termine del periodo di formazione dello specializzando presso lo IOV – IRCCS, sarà cura del direttore/responsabile della Unità Operativa sede della formazione comunicare la cessazione alla UOS Sistemi Informativi – Servizio Abilitazioni affinché vengano disattivate le utenze e le credenziali di accesso.

Art. 16 – Obblighi delle persone che operano all'interno dell'Istituto Oncologico Veneto-IRCCS

Tutte le persone che prestano attività all'interno dello IOV-IRCCS a qualsiasi titolo, con o senza retribuzione, compresi gli allievi e i docenti dei corsi di formazione e di aggiornamento professionale, anche in convenzione con le università, gli specializzandi, i tirocinanti e i volontari, qualora in occasione della loro attività vengano a conoscenza di dati personali trattati dallo IOV sono tenuti a trattare gli stessi in modo da garantirne la sicurezza e la riservatezza, a osservare e rispettare le disposizioni del presente Regolamento e le istruzioni impartite dal Titolare del trattamento e dal Delegato Privacy.
Per le finalità del presente articolo il Delegato del trattamento fornisce le necessarie informazioni alle persone che operano a qualsiasi titolo nella propria struttura.

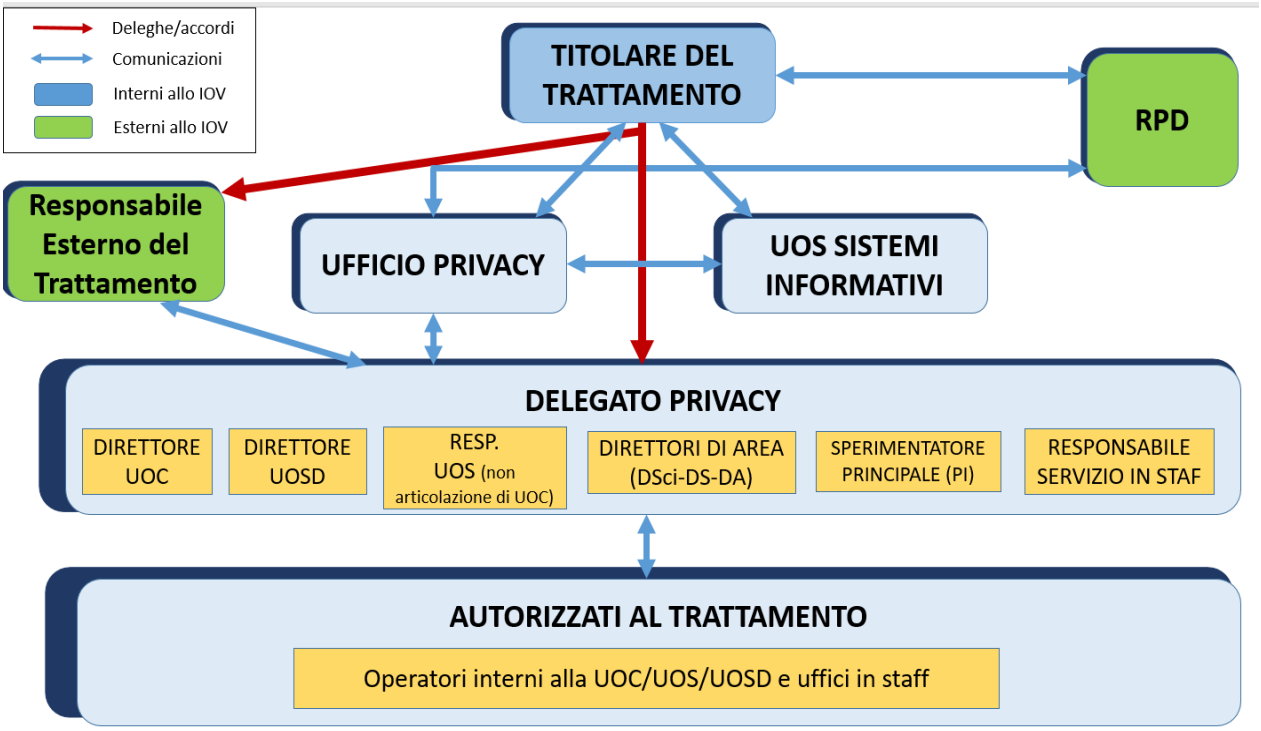

Figura 1–Organigramma privacy IOV

TRATTAMENTO DEI DATI PERSONALI NEI RAPPORTI CON I SOGGETTI TERZI

Art.17 – Configurazione dei ruoli in materia di protezione dei dati personali nei rapporti con i soggetti terzi.

1-In conformità al principio di *accountability* (responsabilizzazione) il Titolare del trattamento pone in essere tutte le misure tecniche ed organizzative idonee a garantire che il trattamento dei dati personali connesso ai rapporti di collaborazione instaurati con soggetti terzi, intesi come le persone fisiche o giuridiche con i quali lo IOV stesso entra in contatto per il perseguimento delle proprie finalità istituzionali sia lecito, legittimo, trasparente, proporzionato alle finalità e sicuro.

2-Per garantire che i rapporti tra lo IOV–IRCCS e i soggetti terzi siano correttamente configurati e disciplinati per quanto attiene ai dati personali, il responsabile del procedimento che attiva la collaborazione con i soggetti terzi valuta:

- il ruolo che rivestirà il soggetto terzo (cliente o fornitore/professionista);
- l'oggetto del contratto/convenzione, per determinare se lo stesso comporti trattamenti di dati personali da parte del soggetto terzo.

3-Nel caso in cui un soggetto terzo, per erogare un servizio o per eseguire la prestazione concordata, debba trattare dati personali in nome e per conto dello IOV-IRCCS utilizzando strumentazione propria oppure portando presso la propria sede i supporti su cui i dati personali sono contenuti, è individuato quale Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679

4-Tale individuazione avviene mediante accordo scritto seguendo lo schema contrattuale predisposto dallo IOV – IRCCS, denominato "Accordo di nomina a responsabile del trattamento", il quale contiene gli elementi elencati nell'art. 28 del GDPR. È compito del responsabile del procedimento/dell'estensore del contratto/convenzione principale integrare il predetto schema di Accordo di nomina con l'indicazione della tipologia dei dati trattati, delle categorie di interessati e delle attività di trattamento che il Responsabile è tenuto a compiere sui dati personali necessari all'esecuzione del contratto/convenzione principale.
Lo schema di accordo di nomina a responsabile del trattamento, insieme con la modulistica necessaria alla gestione dei rapporti con i soggetti terzi, è reso disponibile al personale dello IOV-IRCCS mediante Intranet aziendale e diffuso con i canali di informazione interna.
Il Titolare può delegare la sottoscrizione dell'accordo di nomina a responsabile del trattamento allo stesso Direttore/Responsabile dell'Unità Operativa a cui sia stata delegata la sottoscrizione del contratto o altro negozio giuridico principale collegato alla nomina a responsabile del trattamento.

4-Nel caso in cui il soggetto terzo, per erogare un servizio o per dare esecuzione alla prestazione, debba trattare dati in nome e per conto dello IOV – IRCCS mediante la strumentazione fornita dallo IOV stesso, il personale del soggetto terzo è autorizzato al trattamento dei dati personali dallo IOV– IRCCS. Di tale autorizzazione viene dato atto nel contratto o altro atto giuridico che disciplina la prestazione principale.

5-Per tutti i casi in cui il soggetto terzo e il personale dello stesso non fosse tenuto a svolgere operazioni di trattamento, ma potesse comunque venire a conoscenza di dati personali trattati dallo IOV – IRCCS, sarà cura del responsabile del procedimento/dell'estensore del contratto o altro atto giuridico con cui viene disciplinata l'erogazione della prestazione vincolare il personale del soggetto terzo alla riservatezza.

Art. 18-Contitolarità

Qualora, in ragione di un contratto o di altro accordo giuridico, lo IOV– IRCCS e uno o più soggetti terzi dovessero trattare dati personali stabilendo congiuntamente le relative finalità ed i corrispondenti mezzi di trattamento, tali soggetti saranno qualificati come contitolari.

Di tale circostanza è necessario dare atto nel contratto o altro accordo giuridico stipulato tra lo IOV– IRCCS e il/i soggetto/i terzo/i.

L'Ufficio Privacy, sente il Responsabile della Protezione dei Dati in relazione ai fini di una corretta valutazione in merito alla sussistenza di un rapporto di contitolarità per la quale è necessario verificare che siano state congiuntamente decise:

- le finalità;
- i mezzi di uno specifico trattamento dei dati personali.

L'Ufficio Privacy, con il Responsabile della Protezione dei Dati, fornisce il supporto per la stesura dell'Accordo di contitolarità, alle Unità Operative interne direttamente interessate.

Art. 19- Ulteriori adempimenti

Gli accordi di nomina di responsabile del trattamento unitamente ai contratti/convenzioni

principali sono conservati presso l'Unità Operativa che li ha redatti. Il Delegato Privacy vigila sul corretto adempimento.

Gli Accordi di contitolarità sono conservati presso l'Ufficio Privacy.

DIRITTI DEGLI INTERESSATI

Art.20 – Informativa

Lo IOV– IRCCS, attraverso l'Ufficio Privacy, predispone informative sul trattamento dei dati personali chiare e comprensibili per fornire all'interessato tutte le informazioni relative al trattamento; tali informazioni vengono fornite in forma concisa, trasparente, intelligibile e facilmente accessibile.

L'informativa sul trattamento dei dati personali riporta le informazioni previste dalla normativa vigente relativamente a:

- l'identità e i dati di contatto del Titolare del trattamento e del Responsabile per la Protezione dei Dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- le modalità di trattamento dei dati personali;
- l'obbligatorietà o meno del conferimento dei dati;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- i soggetti destinatari ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- come possono essere esercitati i diritti di accesso in base alle disposizioni vigenti;
- il diritto dell'interessato di chiedere al Titolare l'accesso ai dati personali e la rettifica del trattamento che lo riguarda o di opporsi al loro trattamento;
- qualora la liceità del trattamento dei dati sia basata sul preventivo rilascio di consenso al trattamento, il diritto di revocarlo in qualsiasi momento senza pregiudicare la liceità del trattamento effettuato prima della revoca;
- il diritto di proporre reclamo al Garante per la privacy;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
- nel caso in cui i dati personali non siano stati ottenuti presso l'interessato, la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

L'informativa all'interessato viene resa anche per estratto tramite l'affissione di appositi manifesti o la somministrazione di appositi documenti nei locali di accesso all'utenza.

L'informativa sul trattamento dei dati personali non viene fornita all'interessato da parte dello IOV nel caso in cui lo stesso interessato disponga già delle suindicate informazioni o nel caso in cui comunicarle risulti impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Le informazioni sono fornite per iscritto o con altri mezzi, anche – se del caso – con mezzi elettronici.

Le informative sono pubblicate nel sito istituzionale: https://www.ioveneto.it/privacy/

Art. 21 – Diritti dell'interessato

Gli interessati - o per loro conto il Tutore/Amministratore di Sostegno (AdS)/Curatore/Esercente responsabilità genitoriale - possono contattare lo IOV-IRCCS e il Responsabile per la protezione dei dati per tutte le questioni relative al trattamento dei propri dati personali e per l'esercizio dei propri diritti.

Le richieste di esercizio dei diritti degli interessati nell'ambito delle sperimentazioni cliniche possono pervenire, oltre che al RPD, allo Sperimentatore Principale a cui è affidata la conduzione dello studio clinico, quale Delegato privacy dal Titolare del trattamento, come previsto dall'art. 17 del presente Regolamento.

L'interessato – o per loro conto il Tutore/Amministratore di Sostegno (AdS)/Curatore/Esercente responsabilità genitoriale – ha il diritto di ottenere dallo IOV-IRCCS la conferma che sia o meno in corso un trattamento di dati personali che lo riguarda e, in tal caso, ottenere l'accesso ai dati personali e alle seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi od organizzazioni internazionali;
- il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo al Garante per la privacy;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento.

All'interessato è garantito l'esercizio dei seguenti diritti:

- Il diritto all'oblio: l'interessato ha il diritto di ottenere dal titolare la cancellazione dei dati personali che lo riguardano se sussiste una delle seguenti condizioni:
  - i dati non sono più necessari alle finalità per le quali sono stati raccolti;
  - l'interessato revoca il consenso, se non sussiste altro fondamento giuridico per il trattamento;
  - l'interessato si oppone al trattamento ai sensi dell'art. 21 e non sussiste alcun motivo per procedere al trattamento;
  - i dati devono essere cancellati per legge;
- Il diritto alla portabilità dei dati, che garantisce all'interessato la possibilità di trasmettere i dati da un titolare all'altro.
- il diritto alla limitazione che permette all'interessato di pretendere che il trattamento dei propri dati sia limitato a quanto necessario ai fini della conservazione.

L'interessato ha il diritto di ottenere dallo IOV la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chiunque abbia legittimo interesse, documentato nelle forme di legge, anche mediante delega o procura a persone fisiche o ad associazioni, conferita per iscritto e

nelle forme di legge, fatta salva la volontà espressa, libera e inequivocabile dell'interessato di vietare l'esercizio dei diritti sopra indicati.

Art. 22- Gestione delle istanze per l'esercizio dei diritti dell'interessato

A) Modalità di presentazione

L'istanza di esercizio dei diritti dell'interessato è presentata sia dall'interessato stesso sia dal Tutore/Amministratore di Sostegno (AdS)/Curatore/Esercente responsabilità genitoriale dell'interessato stesso in forma scritta all'ufficio protocollo dello IOV che lo registra e lo assegna in prima istanza all' Ufficio Privacy.

L'interessato, nell'esercizio dei diritti sopra riportati può conferire per iscritto, delega o procura a persone fisiche o ad associazioni.

Qualora l'istanza sia presentata verbalmente, il dipendente o il collaboratore dello IOV-IRCCS invita l'interessato o il Tutore/Amministratore di Sostegno (AdS)/Curatore/Esercente responsabilità genitoriale dell'interessato stesso a compilare il modello di richiesta predisposto dall'Autorità Garante per la Protezione dei Dati Personali e disponibile nella sezione del sito web istituzionale dello IOV-IRCCS dedicata alla modulistica e alla documentazione di interesse dell'Utente.

B) Modalità di valutazione e riscontro delle istanze per l'esercizio dei diritti dell'interessato

Ricevuta l'istanza di esercizio dei diritti, l'Ufficio Privacy valuta l'ammissibilità della stessa in ordine alla fondatezza e alla proporzionalità della richiesta, con il supporto delle Unità Operative interessate.
Se l'istanza è ammissibile, il Direttore della UOC Affari Generali con il supporto dell'Ufficio Privacy e con la collaborazione delle Unità Operative interessate fornisce il riscontro in forma scritta, salvo diversa modalità indicata dall'interessato.
Qualora l'istanza sia ritenuta manifestamente infondata o eccessiva, Il Direttore della UOC Affari Generali, su istruttoria dell'Ufficio Privacy e con il supporto delle Unità Operative eventualmente coinvolte, informa l'interessato o il Ttutore/Amministratore di Sostegno (AdS)/Curatore/Esercente responsabilità genitoriale dell'interessato stesso senza ingiustificato ritardo e, in ogni caso, entro un mese dal ricevimento della richiesta stessa.

C) Termini per il riscontro alle istanze per l'esercizio dei diritti dell'interessato.

Il riscontro deve avvenire senza ingiustificato ritardo e, comunque, al più tardi entro 30 giorni dal ricevimento dell'istanza stessa.
Il termine di 30 giorni può essere prorogato di due mesi, se ciò si rende necessario in ragione della complessità e del numero delle richieste. In tal caso, il Direttore della UOC Affari Generali informa di tale proroga e dei motivi del ritardo, entro un mese dal ricevimento dell'istanza.

Art. 23– Diritto di opposizione

L'interessato - o per suo conto il Tutore/Amministratore di Sostegno (AdS)/Curatore/Esercente responsabilità genitoriale - ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano e l'Istituto si astiene dal trattarli ulteriormente, salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, diritti e libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art.24 – Diritto di accesso alla documentazione e diritto alla riservatezza

L'Istituto, in osservanza delle disposizioni vigenti in tema di riservatezza e di trasparenza valuta, anche con riguardo ad altre regolamentazioni specifiche, la possibilità degli interessati di accedere ai documenti, per il quale ha adottato apposito regolamento pubblicato nel proprio sito istituzionale.
Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, l'accesso ai relativi dati è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

Art.25-Diritto di accesso generalizzato

Nel caso in cui nel corso della procedura di accesso civico ai sensi del D. Lgs. n. 33/2013 venissero in evidenza problematiche connesse alla tutela dei dati personali di soggetti terzi, l'accesso civico generalizzato viene rifiutato laddove possa arrecare un pregiudizio concreto alla protezione dei dati personali in conformità con la disciplina legislativa in materia.
Il Delegato del trattamento dei dati interessato dall'accesso civico generalizzato, sentito il Responsabile della Protezione dei dati e – se del caso – il Responsabile per la trasparenza , dovrà operare la valutazione caso per caso al fine di verificare la sussistenza o meno del pregiudizio nel rispetto della normativa di settore, in particolare delle Linee Guida adottate dall'Autorità Nazionale Anticorruzione d'intesa con il Garante di cui alla delibera n. 1309 del 28/12/2016.

SICUREZZA DEI DATI PERSONALI

Art. 26- Registro delle attività di trattamento dei dati personali

Lo IOV– IRCCS, in qualità di Titolare del trattamento, redige un Registro delle attività di trattamento,-documento che descrive le attività di trattamento svolte sotto la sua autorità.

Oltre al-nome e ai dati di contatto del Titolare del trattamento e del Responsabile della Protezione dei Dati Personali, nel Registro sono annotate le seguenti informazioni;

a) la descrizione delle attività di trattamento e le Unità Operative competenti;
b) ove esistenti, il nome e i dati di contatto del contitolare del trattamento e del responsabile del trattamento;
c) le finalità del trattamento;
d) una descrizione delle categorie di interessati e delle categorie di dati personali;
e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
f) gli eventuali trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e la documentazione che attesta le garanzie adeguate;
g) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
h) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Il registro è mantenuto sempre aggiornato dall'Ufficio Privacy e dalla UOS Sistemi Informativi per la parte di competenza descritta sub art. 13, per garantire che esso corrisponda effettivamente alla realtà dei trattamenti svolti dal Titolare o dal Responsabile del trattamento.
Il Registro è adottato in formato elettronico e consente il tracciamento delle variazioni; ad accedere al registro vengono abilitati l'Ufficio Privacy e la UOS Sistemi Informativi. Sono abilitati alla visualizzazione del Registro i Delegati e il RPD.
.

Art. 27 – Sicurezza del trattamento

Il Titolare, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio.
La gestione, informatica e cartacea, dei dati personali e delle categorie particolari di dati, in particolare dei dati relativi alla salute, costituisce un elemento fondamentale delle attività istituzionali dello IOV–IRCCS che consistono nella diagnosi, nella cura e nella ricerca.
I trattamenti sono svolti nell'osservanza di misure di sicurezza volte a garantire:
- la riservatezza;
- la protezione dalla perdita e dalla distruzione;
- la pronta disponibilità in caso di necessità.

Art.28 -Misure di sicurezza tecniche

1-I sistemi informatici aziendali sono sviluppati in modo tale da garantire la riservatezza, l'integrità e la disponibilità dei dati in essi archiviati.
I soggetti autorizzati al trattamento sono tenuti a conoscere e ad osservare i regolamenti interni, le procedure e le istruzioni operative che prescrivono le corrette modalità di utilizzo dei sistemi informatici aziendali, al fine di prevenire e contenere gli incidenti di sicurezza.
Il Responsabile della UOS Sistemi Informativi redige e aggiorna il Regolamento sul corretto utilizzo dei sistemi informativi aziendali e ne cura la massima diffusione a tutto il personale dello IOV-IRCCS, avvalendosi della collaborazione dei Direttori/Responsabili di Unità Operativa.

2-L'Istituto ha definito una politica di gestione delle autorizzazioni prevedendo che l'accesso ai sistemi operativi, alla posta elettronica e agli applicativi software aziendali avvenga previa assegnazione delle credenziali personali — identificativo dell'utente e password — ad ogni singolo collaboratore, il quale è responsabile delle loro custodia.
L'accesso ai dati personali è limitato ai soli dati necessari allo svolgimento delle mansioni lavorative.

3-La richiesta di abilitazione di ciascun collaboratore ad accedere ai sistemi informativi aziendali è presentata alla UOS Sistemi Informativi mediante apposita modulistica e deve essere sottoscritta dal Delegato al trattamento dei dati personali competente per l'ambito organizzativo a cui l'autorizzato afferisce.

4-L'Istituto valuta le tipologie di trattamento di dati personali e i dispositivi sia hardware che software su cui i dati sono archiviati e provvede a mantenerli aggiornati e protetti, installando sistemi di protezione quali antivirus, firewall e le eventuali patch.

5- I dati personali vengono pseudonimizzati utilizzando appositi software o tecniche di cifratura, conservando la chiave di cifratura in luogo sicuro e ad accesso limitato.

6-Nel caso di trasmissione di dati personali verso l'esterno, l'Istituto utilizza protocolli di trasmissione sicuri che implementino, se del caso, la cifratura.

7- L'Istituto predispone e aggiorna, anche in collaborazione con i fornitori di dispositivi hardware e software, un piano per garantire la continuità operativa delle proprie attività.

Art. 29 – Misure di sicurezza dei documenti e degli archivi cartacei

1-Per quanto attiene al trattamento di dati personali su supporto cartaceo, i soggetti autorizzati devono attenersi alle seguenti misure di sicurezza:
- conservare i documenti in luoghi e contenitori idonei ad evitare perdite, sottrazioni, danneggiamenti e accesso a soggetti non autorizzati;
- obbligo di custodire con diligenza i supporti cartacei contenenti i dati personali per tutto

il periodo in cui si effettuano trattamenti;
- nel caso di allontanamento dalla postazione di lavoro, anche temporaneo, riporre la documentazione in armadi o cassetti o comunque non lasciarla incustodita.

2-La responsabilità della conservazione e della sicurezza degli archivi correnti dei documenti amministrativi contenenti dati personali e collocati all'interno dei locali dello IOV-IRCCS è di ciascun Direttore/Responsabile di Unità Operativa, che li produce e li detiene fino al loro conferimento all'archivio di deposito.

3-La responsabilità della conservazione e della sicurezza degli archivi correnti dei documenti sanitari e collocati all'interno dei locali della singola Unità Operativa è del Direttore/Responsabile della stessa – ad eccezione delle Unità Operative Semplici articolazione di UOC per le quali resta responsabile il Direttore di UOC – e dei coordinatori infermieristici delle stesse che li detiene fino al loro conferimento all'archivio corrente centralizzato o all'archivio di deposito.
Qualora la documentazione sanitaria fosse conservata in locali centralizzati del presidio ospedaliero la responsabilità della corretta gestione e custodia degli stessi è affidata alla Direzione Medica di Ospedale.

4-La gestione dell'archivio di deposito e la conseguente responsabilità della corretta conservazione della documentazione custodita sono affidati al soggetto terzo aggiudicatario del servizio e sono previsti nell'accordo di nomina di responsabile del trattamento allegato al contratto di affidamento del servizio.

5-Il Direttore Sanitario vigila sulla corretta conservazione e sulla modalità di accesso della documentazione sanitaria, conservata in archivi di deposito.

Art. 30 – Violazione dei dati personali

Lo IOV-IRCCS disciplina la gestione degli eventi potenzialmente qualificabili come *data breach* con apposita procedura interna, comunicata a tutti i dipendenti e messa a disposizione degli stessi in intranet seguendo il seguente percorso "*L'azienda informa->Sistema di gestione per qualità->Direzione amministrativa->Privacy->P_Gestione di eventi potenzialmente qualificabili come data breach*", allegata al presente regolamento, fatti salvi eventuali aggiornamenti si rendessero necessari.
La procedura interna prevede i seguenti requisiti:
- la segnalazione tempestiva all'ufficio deputato alla gestione della possibile violazione da parte del soggetto che rileva una possibile violazione;
- la notifica della violazione al Garante per la privacy al ricorrere delle condizioni previste dalla normativa vigente e dalla procedura;
- il contenuto essenziale della notifica della violazione;
- i requisiti della comunicazione all'interessato della violazione.

Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nel registro delle violazioni dei dati gestito dall'ufficio privacy; tale documentazione consente al Garante per la privacy di verificare il rispetto delle disposizioni di legge.

Art. 31 – Limiti alla conservazione dei dati personali

Lo IOV provvede all'adozione di apposite misure e procedure attraverso le quali:
- disciplina la distruzione dei documenti analogici che contengono dati personali, una volta terminato il limite di conservazione degli stessi in conformità al massimario di scarto adottato e previa autorizzazione della Soprintendenza ai beni culturali e dei documenti digitali che contengono dati personali come da manuale di conservazione adottato;

- smaltire gli apparati hardware o supporti rimovibili di memoria con modalità che non rendano possibile accedere ad alcun dato personale di cui è titolare lo IOV;
- assicurare che il riutilizzo degli apparati di memoria o hardware sia effettuato con modalità da garantire che non sia possibile accedere ad alcun dato personale di cui è titolare lo IOV

Art. 32- Valutazione d'impatto (Data Protection Impact Assessment DPIA)

La valutazione d'impatto o *Data Protection Impact Assessment* (DPIA) è un processo volto alla gestione dei rischi per i diritti e le libertà degli interessati connessi al trattamento dei dati personali, mediante l'analisi del contesto del trattamento stesso, la valutazione dei principi di proporzionalità e necessità del trattamento e delle misure previste per gestire i rischi.
Nel caso in cui un trattamento possa comportare, in relazione alla natura, all'oggetto, alle finalità e alle modalità di trattamento, con particolare riferimento all'uso di una nuova tecnologia, un rischio elevato per i diritti e le libertà degli interessati il Titolare effettua la valutazione d'impatto sulla protezione dei dati personali.
Il Titolare consulta il Responsabile Protezione Dati (RPD), il quale fornisce parere sulla valutazione stessa e ne sorveglia lo svolgimento, in merito:

- alla necessità di svolgere la valutazione d'impatto;
- alla metodologia da utilizzare;
- all'individuazione dei soggetti, sia interni sia esterni, da coinvolgere.

L'Ufficio Privacy e la UOS Sistemi Informativi supportano il Titolare nella valutazione d'impatto sulla protezione dei dati personali.
Il RPD e la UOS Sistemi Informativi, ciascuno nel proprio ambito di competenza, propongono al Titolare del trattamento di effettuare la DPIA su specifiche attività di trattamento.

La DPIA viene effettuata raggruppando più trattamenti che siano simili tra loro per contesto, natura, ambito di applicazione, finalità e rischi.

MODALITÁ SPECIFICHE DI TRATTAMETNO DEI DATI PERSONALI

Art. 33- Dossier Sanitario Elettronico

Il Dossier Sanitario Elettronico (DSE) configura un trattamento effettuato tramite strumenti informatici di insiemi di dati e documenti digitali di tipo sanitario generati da eventi clinici riguardanti l'assistito all'interno dello IOV.

Lo IOV– IRCCS ha istituito il proprio Dossier Sanitario Elettronico per la condivisione all'interno dello IOV– IRCCS stesso dei dati sanitari degli utenti al fine di migliorare il percorso di cura.

In ossequio al principio di autodeterminazione, è garantita al paziente la massima libertà di scelta in ordine alla costituzione del DSE attraverso l'espressione di uno specifico consenso raccolto una tantum.

Per assicurare che il consenso alla costituzione del DSE sia libero ed informato, lo IOV– IRCCS mette a disposizione dei pazienti e degli utenti l'informativa sul trattamento dei dati personali effettuato tramite DSE.
L'accesso e la consultazione dei dati contenuti nel DSE è consentito soltanto al personale sanitario coinvolto nel processo cura e a quello amministrativo per le sole finalità strettamente correlate alla cura. Gli accessi e le operazioni svolte sul DSE, anche la semplice consultazione, sono tracciati e registrati automaticamente.
Lo IOV – IRCCS garantisce l'esercizio dei diritti degli interessati, tra cui il diritto di accesso ai dati, il diritto di rettifica e integrazione, attraverso apposita modulistica.

Art. 34 – Redazione degli atti, pubblicità e tutela della trasparenza

I responsabili delle Unità Operative che propongono una deliberazione o che adottano un provvedimento dirigenziale con il supporto tecnico dei relativi responsabili del procedimento verificano, alla luce dei principi di minimizzazione e di proporzionalità sanciti dalla normativa, che l'inclusione nel testo e nell'oggetto di dati personali sia realmente necessaria per perseguire le finalità dell'atto stesso.
Devono essere privilegiate modalità di redazione degli atti che prevedono l'utilizzo di dati resi anonimi o non direttamente identificativi, quali codici o altri riferimenti se lo scopo cui l'atto è preordinato è ugualmente raggiungibile.
L'Istituto garantisce la riservatezza dei dati sensibili in sede di pubblicazione all'Albo on-line delle deliberazioni o di altri provvedimenti amministrativi, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati.

Art. 35 – Obblighi di trasparenza

L'Istituto assolve agli obblighi di legge in materia di trasparenza, quale livello essenziale delle prestazioni concernenti i diritti civili e sociali ai sensi dell'art.117, lettera m) della Costituzione, con la pubblicazione sul proprio sito internet istituzionale dei dati di cui al D. Lgs. n. 33/2013, nel rispetto delle "*Linee Guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*" emanate dal Garante per la protezione dei dati personali il 15.05.2014.

RICERCA SCIENTIFICA E SPERIMENTAZIONI CLINICHE

Art. 36 – Principi generali per il trattamento dei dati personali nell'ambito della ricerca e delle sperimentazioni cliniche

Lo IOV-IRCCS svolge l'attività di ricerca scientifica perseguendo standard di eccellenza nei seguenti ambiti:

- **ricerca clinica:** migliorare la conoscenza delle patologie oncologiche, sviluppare nuovi trattamenti, dispositivi medici e metodi diagnostici per garantire una migliore cura dei pazienti;
- **ricerca epidemiologica**: esaminare la distribuzione delle patologie oncologiche nella popolazione, i fattori di rischio per la loro comparsa e la relazione con abitudini e stili di vita. Inoltre, l'epidemiologia analizza l'efficacia degli esami preventivi e degli screening per la diagnosi precoce, valutando il rapporto tra costi e benefici;
- **ricerca pre-clinica:** nell'ambito di sperimentazioni in vitro e in vivo, volte allo sviluppo di nuovi farmaci, strumenti diagnostici e clinici, nonché al miglioramento e all'elaborazione di nuove strategie per la somministrazione dei farmaci. L'attività di ricerca pre-clinica è strumentale alla ricerca clinica, in quanto sulla base dei risultati ottenuti in questi studi vengono disegnati gli studi clinici di fase I, cioè le prime fasi della sperimentazione nell'uomo che porteranno, dopo anni di attente osservazioni, all'approvazione della nuova terapia e, quindi, al miglioramento dei percorsi di cura offerti ai pazienti;
- **ricerca traslazionale:** valutare la possibilità di trasformare le scoperte scientifiche derivanti dalle ricerche effettuate in laboratorio in applicazioni cliniche per ridurre l'incidenza e la mortalità dovuti alle patologie oncologiche. Tale settore della ricerca permette di utilizzare ed applicare le più recenti scoperte scientifiche, ad esempio nel campo della genetica o della biologia molecolare, alla pratica clinica quotidiana. Momento essenziale della ricerca traslazionale è anche l'osservazione dei pazienti, da cui i ricercatori colgono frequentemente spunti per nuovi esperimenti in laboratorio al fine di migliorare i percorsi di cura offerti.

Il trattamento di dati per finalità di ricerca è reso lecito dall'art. 9, par. 2 lett.j) e dall'art. 89 del Regolamento (UE) 2016/679
Lo IOV– IRCCS raccoglie, ove necessario, il consenso per il trattamento dei dati personali e delle categorie particolari di dati, garantendo che il consenso è libero, facoltativo e preceduto da un'idonea informativa.
Il principio di trasparenza impone che i dati personali siano trattati in modo corretto e trasparente nei confronti dell'interessato, il quale deve essere informato dal Responsabile del progetto scientifico individualmente dell'esistenza del trattamento e del fatto che suoi dati personali e delle categorie particolari di dati sono trattati a fini scientifici.

Art. 37 – Trattamento dati nelle sperimentazioni cliniche

L'Istituto svolge le attività relative alle sperimentazioni cliniche di farmaci e di dispositivi medici in ottemperanza alle *Good Clinical Practice* e attenendosi alle Linee Guida del Garante per la Protezione dei Dati Personali per il trattamento dei dati nelle sperimentazioni cliniche del 24 luglio 2008.
Duplice è l'obiettivo perseguito attraverso l'attività di ricerca clinica che unisce la tutela della salute alla ricerca, fissando nel contempo standard di qualità e sicurezza dei medicinali grazie alla robustezza dei risultati che scaturiscono dall'analisi degli studi clinici.

In qualità di Istituto di Ricovero e Cura a Carattere Scientifico, il trattamento di dati personali per la conduzione di sperimentazioni cliniche da parte dello IOV è necessario per l'esecuzione di un compito di interesse pubblico nel settore della sanità pubblica.
Lo IOV – IRCCS raccoglie, tramite lo Sperimentatore Principale delegato dal Titolare, il consenso dell'interessato al trattamento dei dati personali necessari alla conduzione della sperimentazione clinica, avendo cura che il consenso stesso sia esplicito, libero, inequivocabile e consapevole. A tal fine viene consegnata all'interessato idonea informativa in cui sono descritte le modalità di trattamento dei dati nell'ambito del singolo studio.
I rapporti tra lo IOV – IRCCS e i soggetti terzi coinvolti nelle sperimentazioni cliniche (a titolo esemplificativo, Promotori, centri partecipanti, *Contract Research Organization*) relativi al trattamento dei dati personali sono disciplinati da apposita clausola contrattuale che specifica i ruoli rivestiti da ciascuna delle parti coinvolte in una sperimentazione clinica.
Le Parti si obbligano al rispetto della normativa in materia di protezione dei dati personali, impegnandosi a dissociare i dati identificativi dei pazienti arruolati nella sperimentazione clinica dai dati relativi allo studio in modo tale che siano trasmessi solo dati pseudonimizzati, a rendere idonea informativa ai pazienti stessi e a raccogliere il consenso al trattamento dei dati per quanto attiene alla sperimentazione stessa, ad adottare le misure logiche e organizzative necessarie a garantire la sicurezza del trattamento.
In tale ambito lo IOV, in qualità di Titolare, si avvale dello strumento della delega di funzioni, per attribuire le competenze e le responsabilità in materia di protezione dei dati personali e i relativi compiti, oltre a quelli ulteriori legati alla specifica attività, a ciascun Responsabile Scientifico/ Sperimentatore Principale volta per volta individuato nel provvedimento autorizzatorio per ciascun progetto di ricerca/sperimentazione clinica.
Al fine di tutelarne l'integrità e la riservatezza, i dati personali e di quelli appartenenti alle categorie particolari di dati dei pazienti arruolati vengono trattati utilizzando tecniche di pseudonimizzazione.
Lo sperimentatore principale conserva e custodisce la chiave di decifratura in modo da evitare la divulgazione non autorizzata o la perdita della stessa.
Allo Sperimentatore Principale, individuato nel provvedimento che autorizza la sperimentazione clinica, sono delegati con apposito atto scritto i compiti in materia di protezione dei dati personali con riferimento allo studio affidato alla sua conduzione.

DISPOSIZIONI FINALI

Art. 38- Formazione

L'Istituto organizza, di norma nell'ambito del piano annuale di formazione del personale, interventi di formazione e aggiornamento in materia di tutela della riservatezza e protezione dei dati personali, finalizzati alla conoscenza delle norme, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni ai dati stessi.

Art. 39- Norma di rinvio

Per tutto quanto non previsto dal presente Regolamento si rinvia alla normativa comunitaria, statale e regionale in materia, nonché ai provvedimenti emanati dal Garante per la privacy.

Specifiche disposizioni si trovano nelle procedure e nei regolamenti aziendali adottati dall'Istituto in elenco:

- Regolamento concernente il corretto utilizzo dei sistemi informativi;
- Procedura per la gestione degli eventi potenzialmente qualificabili come *data breach*;
- Massimario di scarto per gli archivi;
- Manuale Aziendale relativo alla gestione documentale;
- Regolamento in materia di diritto di accesso agli atti;
- Piano triennale per la prevenzione della corruzione e della trasparenza.

Art-40- Entrata in vigore

Il presente Regolamento entra in vigore il giorno successivo a quello della pubblicazione della relativa deliberazione di approvazione nell'Albo on-line istituzionale.