CENTRO NEUROLESI BONINO PULEJO
IRCCS MESSINA

REGOLAMENTO

Per la protezione dei dati personali

(Regolamento Europeo 2016/679, D. Lgs. 196/2003 modificato dal D. Lgs 101/2018)

Il Commissario Straordinario
Dott. Vincenzo Barone

ALLEGATO ALLA DELIBERA N. 119/CS DEL 29/1/2019

Sommario

PREMESSA

Il diritto alla protezione dei dati è un vero e proprio diritto inviolabile della persona che non si limita alla tutela della riservatezza o alla privacy, ma implica il pieno rispetto dei diritti e delle libertà fondamentali.

Dall'esame della materia emerge come sia, ormai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle strutture sanitarie, di una riservatezza totale dal punto di vista reale e sostanziale.

Per questi motivi la cultura della privacy necessita di crescere e rafforzarsi, principalmente fra gli operatori della sanità, perché solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di legge, nel trattamento di dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della Qualità del rapporto con l'Utenza.

Il presente regolamento è redatto nel rispetto del **Regolamento Europeo 2016/679** di seguito anche detto **"RGPD"**, Regolamento Generale Protezione Dati, del **D.lgs. n.196/03 modificato dal D. Lgs n.101/2018** di seguito anche detto **"Codice della Privacy"**, nonché dalle Autorizzazioni, e dai Provvedimenti dell'Autorità Garante della Privacy. Rappresenta un atto d'indirizzo in materia di protezione dei dati personali trattati dall'**IRCCS Centro Neurolesi Bonino Pulejo di Messina**, di seguito anche detto **"IRCCS"**. Le istruzioni contenute costituiscono una serie di prescrizioni atte a garantire la sicurezza dei dati e delle informazioni detenute, a vario titolo, dai Presidi Ospedalieri, dalle sedi Spoke e dagli uffici amministrativi.

Considerato che le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali, tecnici, nonché in responsabilità, che il Titolare del Trattamento dei dati personali deve osservare per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy e che l'ordinamento nazionale ha emanato il decreto legislativo di recepimento della sopracitata normativa ad integrazione e modifica di quella esistente, si rende necessario elaborare un Regolamento interno a norma dell'art. 6 del RGPD, degli artt. 2 ter e 2 sexies del D. Lgs 196/2003 modificato dal D. Lgs n. 101/2018.

Capo I Disposizioni Generali

Art. 1 - Oggetto

Il presente Regolamento disciplina il trattamento dei dati personali effettuato dall'IRCCS, secondo quanto previsto dalla normativa vigente. Tale disciplina è diretta a garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche e

giuridiche, con particolare riferimento alla riservatezza e al diritto alla protezione dei dati personali degli utenti e di tutti coloro che hanno rapporti con l'Istituto.

Art. 2 - Definizioni

1) **«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;

2) **«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;

3) **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) **«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;

5) **«pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali 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;

6) **«archivio»**: 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;

7) **«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;

8) «**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;

9) «**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;

10) «**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;

11) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «**violazione dei dati personali**»: 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;

13) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «**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;

15) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «**Autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

17) «**Autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a)il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b)gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c)un reclamo è stato proposto a tale autorità di controllo.

Art.3 - Principi applicabili al trattamento dei dati personali

I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) 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, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento UE a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) 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 («integrità e riservatezza»).

Il titolare del trattamento è competente per il rispetto del presente articolo ed in grado di comprovarlo («responsabilizzazione»).

Art. 4 - Liceità del trattamento

Il trattamento dei dati personali è lecito solo se e nella misura in cui ricorre almeno una delle

seguenti condizioni (art. 6 del Regolamento UE 2016/679):

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. Tale condizione non si applica al trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Il trattamento delle categorie particolari di dati personali di cui all'articolo 9 del Regolamento (UE) 2016/679 (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) è consentito qualora si verifichi uno dei casi riportati al paragrafo 2 del medesimo articolo:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche,
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
e) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

f) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

g) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale

h) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

i) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Art. 5 - Finalità del trattamento

Il trattamento dei dati personali è effettuato dall'IRCCS, in quanto soggetto pubblico, per lo svolgimento dei compiti del Servizio Sanitario Nazionale annoverati tra le finalità di rilevante interesse pubblico ed per l'espletamento delle funzioni istituzionali assegnate e previste dalle normative vigenti.

I trattamenti sono finalizzati all'erogazione delle prestazioni sanitarie nonché agli adempimenti amministrativi e contabili, di organizzazione e di controllo, con particolare riguardo alle attività di:

a) erogazione di prestazioni sanitarie, sia istituzionali che in libera professione (comprensive di tutte le attività di supporto), erogate in regime di ricovero, ordinario o diurno, di assistenza specialistica ambulatoriale, di Day Service o altre modalità, volte alla tutela della salute e dell'incolumità fisica degli utenti, di terzi e della collettività;

b) svolgimento di funzioni di didattica, formazione e ricerca scientifica, statistica ed

epidemiologica, finalizzate alla tutela della salute;

c) tutela della sicurezza e della salute dei lavoratori e sorveglianza igienico-sanitaria delle proprie strutture;

d) esercizio delle funzioni amministrative di competenza dell'Istituto:

   1. La gestione del personale dipendente, comprese le procedure di assunzione;
   2. la gestione dei soggetti che intrattengono rapporti giuridici con l'Istituto, diversi dal rapporto di lavoro dipendente e che operano a qualsiasi titolo all'interno dell'Istituto stesso, ivi compresi gli specializzandi, gli allievi e i docenti di corsi, i tirocinanti, i volontari;
   3. la gestione dei rapporti con i consulenti, fornitori per l'approvvigionamento di beni di servizi nonché con le imprese per l'esecuzione di opere edilizie e di interventi di manutenzione;
   4. la gestione dei rapporti con i soggetti accreditati o convenzionati;
   5. gestione del contenzioso, specificatamente dei rapporti con l'Autorità Giudiziaria e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti;

e) Sono altresì effettuati i trattamenti di dati personali previsti da norme legislative e regolamentari concernenti: l'adempimento di un obbligo legale al quale è soggetto l'IRCCS; per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 6 – Categorie di dati

L'IRCCS tratta dati di tipo personale e particolare relativi a:

- utenti, assistiti, pazienti e loro familiari e/o accompagnatori
- personale sanitario, amministrativo, tecnico e professionale della dirigenza e del comparto in rapporto di dipendenza, convenzione o collaborazione;
- personale universitario che svolge attività assistenziale, di ricerca e di didattica all'interno dell'IRCCS;
- soggetti che per motivi di studio, tirocinio, stage o volontariato frequentano le strutture dell'IRCCS ed effettuano trattamento di dati personali, quali specializzandi, allievi tirocinanti, volontari, ecc;
- clienti e imprese che intrattengono rapporti con l'IRCCS per l'approvvigionamento di beni e servizi o per l'esecuzione di opere edilizie e interventi di manutenzione;
- personale e imprese partecipanti a bandi, gare e selezioni.

I dati personali trattati dall'IRCCS nelle forme e nei limiti di quanto previsto dalla vigente normativa sono raccolti:

- prioritariamente presso l'interessato o anche presso persone diverse nei casi in cui questi sia minorenne o incapace o non sia in grado di fornirli;
- anche presso enti del SSN, presso altri enti e amministrazioni pubbliche o terzi, presso pubblici registri o presso altri esercenti le professioni sanitarie.

Art. 7 - Limiti alla conservazione dei dati personali

L'IRCCS assicura l'adozione di apposite misure e procedure attraverso le quali:

- si proceda alla distruzione dei dati personali secondo le modalità previste dalla legge e una volta terminato il limite minimo di conservazione dei documenti analogici e digitali e dei dati personali ivi riportati;
- siano smaltiti gli apparati hardware o supporti rimovibili di memoria con modalità che non rendano possibile accedere ad alcun dato personale di cui è titolare l'Istituto.
- il riutilizzo di apparati di memoria o hardware sia effettuato con modalità tali da assicurare che non sia possibile accedere ad alcun dato personale di cui è titolare l'IRCCS.

Art. 8 - Le operazioni di trattamento

Per trattamento si intende qualunque operazione, o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicati a dati personali o insiemi di dati personali, come:

- la raccolta dei dati;
- la registrazione dei dati, ovvero il loro inserimento su supporti, automatizzati o manuali, al fine di rendere i dati disponibili per successivi trattamenti;
- l'organizzazione dei dati, cioè il processo di lavorazione finalizzato a favorirne la fruibilità attraverso l'aggregazione, la disaggregazione, l'accorpamento, la catalogazione, ecc.;
- la conservazione dei dati;
- l'adattamento o la modifica in relazione a variazioni o a nuove acquisizioni;
- l'estrazione;
- la consultazione;
- l'uso;
- la comunicazione, ovvero la trasmissione dei dati a uno o più soggetti determinati, in qualunque forma, anche mediante messa a disposizione o consultazione; la comunicazione dei dati avviene

solo nei casi previsti da norme di legge o regolamento;

- la diffusione, ovvero il dare conoscenza dei dati personali a soggetti indeterminati (es. pubblicazione nell'albo pretorio, ecc);
- la limitazione, cioè il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- la cancellazione;
- la distruzione.

Le operazioni di trattamento possono essere effettuate solo dal titolare e dal personale autorizzato. Non è consentito il trattamento da parte di persone non autorizzate.

E' compito degli Autorizzati al trattamento di effettuare la valutazione periodica della non eccedenza dei dati trattati.

Art. 9 - Informazione trasparente

L'IRCCS, quale titolare del trattamento, adotta misure appropriate per fornire all'interessato tutte le informazioni e comunicazioni riguardanti il trattamento dei dati in forma concisa, trasparente intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni rivolte specificatamente ai minori.

Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

L'IRCCS a tal riguardo predispone specifiche informative sul trattamento dei dati personali che riportano le informazioni previste dalla vigente normativa secondo quanto disposto dagli artt. 13 e 14 del R. Europeo 2016/679 relativamente a:

a) identità e i dati di contatto del titolare del trattamento e del Responsabile della Protezione dei Dati;
b) finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
c) destinatari cui possono essere comunicati i dati;
d) periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento;
f) revoca del consenso in qualsiasi momento senza pregiudizio per la liceità del trattamento basata sul consenso prestato prima della revoca;
g) diritto di proporre reclamo al Garante della Privacy;

h) comunicazione di dati personali basata su un obbligo legale o contrattuale;

i) 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;

j) 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 fornita per iscritto, anche per estratto, tramite materiale informativo reso disponibile in luoghi comuni dell'IRCCS e presso l'apposita sezione del portale web www.irccsme.it.

Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente dell'IRCCS, è predisposta separata informativa.

L'informativa sul trattamento dei dati personali non viene rilasciata all'interessato nel caso in cui questi 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, purché in tali casi siano state adottate preventivamente misure tecniche e organizzative adeguate per la protezione dei dati specie al fine di garantire il rispetto del principio della minimizzazione dei dati, e ulteriori misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato.

Qualora l'IRCCS intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente

CAPO II Soggetti del Trattamento

Art. 10 - Titolare del trattamento

L'IRCCS Centro Neurolesi Bonino Pulejo, rappresentato ai fini previsti dal RGPD dal Legale Rappresentane pro tempore (Direttore Generale o Commissario Straordinario) è il **Titolare del trattamento** dei dati personali trattati con strumenti elettronici e cartacei (di seguito indicato con "Titolare"). Il rappresentante legale può delegare le relative funzioni al **Personale autorizzato** a norma dell'art. 2- quaterdecies del Codice della Privacy in possesso di adeguate competenze.

Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di

dimostrare che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del RGPD, nonché dal Capo III della Parte I del Codice della Privacy.

Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato. Le informazioni saranno rese con le modalità e condizioni previste dagli artt. 77, 79, 80, 82 del Codice della privacy.

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ed è inserito nel Provvedimento del Garante della Privacy pubblicato in G. U. il 19/11/2018, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA') ai sensi dell'art.35 RGDP, considerati: la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 25. La stessa valutazione deve essere fatta nel rispetto dell'art. 110 del Codice della privacy, nel caso della ricerca medica, biomedica ed epidemiologica.

Il Titolare, inoltre, nel caso di trattamenti effettuati per suo conto, provvede a designare i Responsabili del trattamento a norma dell'Art. 28 del RGPD che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate. Nel caso di esercizio associato di funzioni e servizi, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

Designa il Responsabile della Protezione dei dati (D.P.O.) di cui agli artt. 37-39 R.E.

Redige, custodisce ed aggiorna il Registro delle attività di trattamento effettuate sotto la propria responsabilità a norma dell'art. 30 del R.E. 2016/679;

Provvede alla notifica all'autorità di controllo in caso di violazione dei dati personali art. 33 R.E. 2016/679

Art. 11 – L'interessato

L'interessato (*data subject*) al trattamento è la **persona fisica** cui si riferiscono i dati personali. La normativa attribuisce specifici diritti all'interessato, il quale, per l'esercizio di tali diritti, può rivolgersi

direttamente al Titolare del trattamento attraverso l'apposita modulistica che potrà essere richiesta presso l'URP oppure scaricata dal sito Internet dell'Istituto all'indirizzo www.irccsme.it. Può esercitare i suoi diritti anche in un momento successivo a quello in cui ha prestato il consenso, potendo così revocare un consenso già prestato.

Art. 12 - Comunicazione di dati all'interessato

I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato mediante consegna diretta allo stesso o con autorizzazione scritta e specifica dell'interessato, mediante consegna a persona dal medesimo delegata per iscritto con indicazione di un documento di riconoscimento in corso di validità nel rispetto delle modalità previste dalla normativa.

Art. 13 - Diritto di accesso dell'interessato

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni (art. 15 Regolamento UE 2016/679):

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato 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;
f) il diritto di proporre reclamo al Garante della Privacy;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate relative al trasferimento.

L'IRCCS fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie

richieste dall'interessato, l'IRCCS può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Art. 14 - Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Art. 15 - Diritto di cancellazione

L'interessato, fatti salvi i casi di esclusione previsti dalla legge, ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento.

Art. 16 - Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano e l'IRCCS si astiene dal trattarli ulteriormente salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici l'interessato ha il diritto di opporsi al trattamento di dati personali che lo riguardano nel rispetto delle

disposizioni previste dal R.E. all'art.89 par. 2 e dal Codice della Privacy 196/2003 come modificato dal D. Lgs 101/2018 art 106 lett. F.

Art. 17 - Diritto alla portabilità dei dati

Nei casi di trattamento effettuato con mezzi automatizzati, l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano. Nell'esercitare il proprio diritto l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

Art.18 - Responsabile della protezione dati

Il Responsabile della Protezione dei Dati, o Data Protection Officer, è designato dall'Istituto in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.

L'IRCCS con deliberazione n.138/CS del 21/5/2018 ha provveduto, in ottemperanza al citato art. 37 e ss. RGDP al conferimento dell'incarico di Responsabile della protezione dei dati, ricorrendo ad una figura esterna, individuata con procedura selettiva.

Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre disposizioni vigenti relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e agli Autorizzati (responsabili interni e incaricati) al trattamento: i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento (art. 28 RGDP). c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di particolarizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a:

-se condurre o meno una DPIA;

-quale metodologia adottare nel condurre una DPIA;

-se condurre la DPIA con le risorse interne ovvero esternalizzandola;

-quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle

persone interessate;

-se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

e) cooperare con l'Autorità Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e dal Responsabile del trattamento al Garante Privacy.

f) tenere i registri di cui ai successivi artt. 24, 26 del presente regolamento;

g) dare supporto al Titolare del trattamento alla predisposizione, di concerto con i responsabili dei servizi interessati, della modulistica, delle linee-guida, delle procedure, delle disposizioni operative, e dei registri e policy necessari a rendere operative le indicazioni di legge e del presente documento.

2. Il Titolare ed il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine il RPD è invitato:

- a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili che abbiano per oggetto questioni inerenti la protezione dei dati personali;

-il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

-il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;

-il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

3. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

4. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente. Coordina l'Ufficio Privacy e ne indirizza le attività.

5. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- il Responsabile del trattamento;
- l'IT Manager o figura equipollente
- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

6. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

Fermo restando l'indipendenza nello svolgimento di dette attività, il RPD riferisce direttamente al Titolare o suo delegato o al Responsabile del trattamento. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

Art. 19 - Responsabile esterno del trattamento

Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo.

La nomina dei Responsabili esterni avviene con contratto o accordo quadro firmato dal Titolare o da un suo delegato per iscritto. Gli originali sono custoditi dal Titolare o dal delegato e copia viene inviata all'Ufficio Privacy che aggiorna l'elenco dei Responsabili esterni anche per permettere al D.P.O. eventuali audit.

E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo dal personale autorizzato che opera sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati trasmessi o comunque trattati.

Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

Il Responsabile si impegna inoltre ai sensi dell'art. 28.3 lett. F, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a prestare ogni necessaria collaborazione al titolare in relazione agli adempimenti degli obblighi sullo stesso gravanti, di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati a norma dell'art. 34. La comunicazione dovrà avvenire a mezzo PEC all'indirizzo azienda@pec.irccsneurolesiboninopulejo.it.
Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinnanzi all'Autorità di controllo o all'Autorità Giudiziaria che riguardano il trattamento dei dati di propria competenza.
La designazione a Responsabile non comporta alcun diritto per questi ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del contratto principale stipulato con l'IRCCS.

Art. 20 - Personale autorizzato al trattamento dei dati personali

I **soggetti autorizzati al trattamento dei dati personali** (SATD) sono le persone fisiche che effettuano le operazioni di trattamento dei dati personali, formalmente designati a tale scopo dal Titolare o dai Responsabili del trattamento i quali forniscono loro per iscritto istruzioni operative dettagliate e specifiche sulle corrette modalità di trattamento che potranno essere integrate in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabili in materia di Protezione dei dati. Possono essere autorizzati secondo profili differenti di responsabilità che dovranno inequivocabilmente evincersi dall'atto di designazione. Il Titolare potrà delegare un Autorizzato al trattamento (a titolo esemplificativo un Autorizzato/Responsabile interno alla designazione di altri Autorizzati (Autorizzati/Incaricati). In questo caso, la delega alla nomina dovrà essere contenuta nell'atto di designazione e riportata nell'atto di nomina dell'Autorizzato/Incaricato.
Possono essere altresì autorizzati i soggetti che a qualsiasi titolo (ad esempio: tirocinanti, studenti, stagisti, volontari, libero professionisti, borsisti, consulenti, ecc.), prestino la loro opera, anche in via temporanea, all'interno delle strutture dell'IRCCS in attività che comportano il trattamento di dati personali per conto dell'IRCCS.
Tutti i soggetti incaricati del trattamento dei dati:

- trattano i dati osservando le istruzioni ricevute, anche con riferimento agli aspetti relativi alla sicurezza;
- svolgono le operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento dei dati personali è consentito;
- qualora trattino dati con l'ausilio di strumenti informatici sono personalmente responsabili della gestione riservata della password loro assegnata, ed è fatto loro divieto di cedere la propria password ad altri;

- sono responsabili della custodia riservata dei documenti cartacei loro affidati per effettuare le operazioni di trattamento e hanno l'obbligo di restituirli al termine delle operazioni loro affidate;
- conservano i dati personali su supporto analogico o digitale solo per il tempo previsto dalla normativa vigente per poi successivamente sottoporli a scarto d'archivio o distruzione;
- non permettono il trattamento dei dati personali che, anche a seguito di verifica, risultino eccedenti o non pertinenti o non necessari, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.
- Devono comunicare al DPO, quando questi ne faccia richiesta, ogni notizia rilevante ai fini dell'osservanza degli obblighi previsti dagli artt. da 32 a 36 del GDPR.
- Fornire al DPO le informazioni utili all'aggiornamento del registro dei trattamenti
- Informare il Titolare del trattamento, senza ingiustificato ritardo della conoscenza dell'avvenuta violazione dei dati.

Art 21 - Amministratore di sistema

L'IRCCS nomina il proprio amministratore di sistema previa valutazione dell'esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e di sicurezza. La designazione è individuale mediante apposito atto e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

L'Amministratore di sistema:

- procede all'adozione di idonee misure di sicurezza dei sistemi informativi dell'Istituto;
- Rilascia le credenziali iniziali agli incaricati del trattamento per l'accesso alle banche dati;
- Vigila affinché l'accesso alle banche dati sia consentito solo al personale allo scopo autorizzato;
- Fornisce supporto al titolare e ai responsabili del trattamento per l'individuazione, applicazione ed aggiornamento delle necessarie misure di sicurezza;
- Svolge ogni altro specifico compito previsto da leggi o regolamenti.

L'IRCCS applica quanto previsto dal provvedimento del Garante della protezione dei dati personali del 27 novembre 2008, modificato con provvedimento del 25 giugno 2009 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

Capo III Adempimenti e misure tecnico organizzative

Art. 22 - Misure organizzative per la tutela della riservatezza

Presso tutti i presidi dell'IRCCS sono adottate procedure atte a garantire la riservatezza degli utenti quali:

- adozione di distanze di cortesia presso gli sportelli;
- divieto di esporre nei reparti o in altri locali aperti al pubblico liste di pazienti in attesa di intervento;
- divieto di chiamare per nome ad alta voce i pazienti in attesa del proprio turno;
- riservatezza nei colloqui con pazienti o familiari evitando di fornire notizie particolari in situazioni di promiscuità o in presenza di personale estraneo o non autorizzato;
- uso nei reparti di terapia intensiva di paraventi o simili al fine di limitare la visibilità del malato ai soli familiari o conoscenti;
- divieto di pubblicare dati personali di pazienti (nomi, foto, ecc.) sulle pagine di social network.

Art. 23 - Autorizzazione al trattamento dei dati personali

Qualora il trattamento dei dati personali sia basato sul rilascio del preventivo consenso da parte dell'interessato, è compito dell'IRCCS dimostrare che questi ha prestato il proprio consenso libero e informato al trattamento dei dati personali.

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

L'interessato ha il diritto di revocare il proprio consenso al trattamento dei dati personali in qualsiasi momento e ciò non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

Il Titolare assicura attraverso idonee modalità l'archiviazione dei consensi espressi dagli interessati in modo da rendere fruibili e rintracciabili le autorizzazioni da questi rilasciate.

Nel trattamento dei dati personali o particolari, effettuati per il perseguimento di finalità di tutela dell'incolumità fisica e della salute dell'interessato, l'IRCCS organizza modalità atte a facilitare l'espressione del consenso da parte dell'interessato, secondo le modalità e le forme previste dalla normative vigente.

In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, stato di necessità o situazione di emergenza sanitaria, il consenso può intervenire senza ritardo, successivamente alla prestazione, da parte di chi esercita legalmente la potestà o da parte di terzi

legittimati.

Il consenso deve essere reso, da parte dell'interessato, attraverso la compilazione di un apposito modello disponibile sul sito web dell'IRCCS o presso il ticket o i reparti, previa consegna e presa d'atto dell'informativa. La manifestazione del consenso verrà resa dall'interessato al momento del primo accesso o, in alternativa, in qualunque altro accesso successivo al primo, e sarà valido ed efficace fino alla revoca dello stesso o, per i minorenni, fino al compimento del diciottesimo anno d'età.

L'eventuale rifiuto a prestare il consenso al trattamento dei dati per finalità di tutela della salute, fatti salvi i casi di urgenza/emergenza sanitaria o di necessità, comporta l'impossibilità di erogazione della prestazione sanitaria richiesta e di ciò va fornita apposita informazione al paziente. Il consenso al trattamento dei dati è valido in relazione alla totalità dei trattamenti dei dati effettuati nell'ambito dell' IRCCS.

Art. 24 - Registro delle attività di trattamento dei dati personali

L'Istituto tiene un registro delle attività di trattamento svolte sotto la propria responsabilità, costantemente aggiornato, che evidenzia i diversi livelli di responsabilità attribuiti in relazione al trattamento dei dati, suddivisi per Autorizzati/Responsabili interni del trattamento, Autorizzati/Incaricati ed Amministratori di Sistema e contiene almeno le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali:
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi gli eventuali destinatari di paesi terzi od organizzazioni internazionali;
e) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
f) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Tale Registro viene tenuto anche dal Responsabile della Protezione dei dati.

Il Registro è tenuto in forma scritta, anche in formato elettronico e, su richiesta, viene messo a disposizione dell'Autorità Garante della Privacy.

Art. 25 - Valutazioni d'impatto sulla protezione dei dati e la consultazione preventiva

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un elevato rischio per i diritti e le libertà delle persone fisiche, l'IRCCS, prima di procedere al trattamento dei dati personali, effettua una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali consultandosi con il

Responsabile della Protezione dei Dati. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi analoghi. La DPIA sarà condotta in tutti quei casi previsti dal Provvedimento del Garante pubblicato in Gazzetta ufficiale n°269 del 19/11/2018

La valutazione contiene almeno:

1. una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dall' IRCCS;
2. una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
3. una valutazione dei rischi per i diritti e le libertà degli interessati;
4. le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento UE, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
5. Se necessario l'IRCCS procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.
6. Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio, l'IRCCS prima di procedere al trattamento consulta il Garante della Privacy, avvalendosi del supporto del DPO.

Art. 26 - Violazione dei dati personali

Una violazione di dati personali è: *ogni infrazione alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento.* La violazione di dati è un tipo particolare di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il Titolare deve identificare l'incidente di sicurezza in genere e comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente ci sono dati personali, particolari, giudiziari. Si possono distinguere tre tipi di violazioni:

1) Violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.

2) Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.

3) Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

In particolari circostanze le violazioni potrebbero essere combinate tra loro.

Ogni SATD è tenuto ad informare senza ingiustificato ritardo l'IRCCS del possibile caso di violazione dei dati personali (data breach).

Ogni interessato, utilizzando l'apposita modulistica può segnalare al titolare del trattamento dei dati un possibile caso di violazione dei dati personali. In tali casi l'IRCCS avvia le necessarie procedure e, avvalendosi della collaborazione dei Responsabili del trattamento, accerta l'effettivo stato dell'arte.

L'IRCCS provvede a notificare la violazione all'Autorità Garante della Privacy senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli Interessati. Qualora la notifica non sia effettuata entro 72 ore, questa è corredata dei motivi del ritardo.

La notifica della violazione dei dati personali deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

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; tale documentazione consente al Garante per la Privacy di verificare il rispetto delle indicazioni di legge.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati a questi viene inoltrata, senza ingiustificato ritardo, apposita comunicazione dell'avvenuta violazione nei modi previsti dalla normativa vigente, salvo i casi di esclusione previsti dalla normativa.

Valutata la necessità di effettuare o meno la notifica della violazione dei dati, l'IRCCS Neurolesi di Messina, procede senza ritardo secondo le modalità stabilite dagli artt. 33 e 34 del GDPR.

Indipendentemente dalla necessità della comunicazione all'Autorità di controllo ed all'interessato, il Titolare provvede a stilare un Registro di Data Breach, tenuto anche dal Responsabile delle Protezione dei dati, contenente:

- il numero della violazione;
- la data della violazione;

- la natura della violazione;
- la categoria degli interessati;
- la categoria dei dati coinvolti;
- le conseguenze della violazione;
- le contro misure adottate;
- la comunicazione o meno al Garante ed all'interessato.

Art. 27 - Misure di sicurezza del trattamento

Il titolare del trattamento ed i responsabili del trattamento dei dati sono tenuti ad adottare, così come previsto dalle disposizioni vigenti in materia di protezione dei dati e di amministrazione digitale, ogni misura di sicurezza necessaria per assicurare un livello sufficiente di sicurezza dei dati personali trattati.

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 varia probabilità e gravità per i diritti e le libertà delle persone fisiche, l'IRCCS mette in atto di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e/o la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

Nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Tutti coloro che trattano dati per conto dell'IRCCS possono trattare dati personali solo se autorizzati e istruiti in tal senso dall'IRCCS stessa.

L'accesso ad ogni procedura informatica è consentito solo se congruente con il trattamento dei dati per il quale si è stati formalmente autorizzati ed è consentito soltanto utilizzando apposite credenziali di autorizzazione fornite dall'IRCCS strettamente personali e della cui riservatezza risponde personalmente il singolo soggetto autorizzato al trattamento dei dati personali.

In caso di trattamenti affidati a soggetti esterni all'IRCCS, i responsabili del trattamento sono tenuti ad assicurare al titolare del trattamento di aver adottato, prima di effettuare ogni attività di trattamento

dei dati, ogni misura minima di sicurezza prevista dalla normativa vigente in materia di protezione dei dati e di amministrazione digitale.
I nominativi ed i dati di contatto del Titolare o dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'IRCCS: www.irccsme.it.

Art. 28 - Attività di verifica e controllo

L'IRCCS definisce apposite modalità per lo svolgimento di attività di verifica e controllo, anche periodico, del rispetto delle misure di legge e delle ulteriori disposizioni in materia di trattamento dei dati personali.
I controlli e le verifiche sono effettuati periodicamente o in caso di necessità anche su sollecitazione degli interessati e le relative attività sono svolte dal personale a ciò incaricato sotto il coordinamento del DPO.

Art. 29 – Formazione

L'IRCCS, nel rispetto dell'art. 32 del GDPR "Sicurezza del trattamento" paragrafo 4 che prevede che *"il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se* **non è istruito in tal senso dal titolare del trattamento"** propone ai propri collaboratori delle sedute formative periodiche per promuovere la cultura della protezione dei dati e per l'aggiornamento informatico giuridico conseguente alle diverse modalità di trattamento. Le attività di formazione possono prevedere anche dei focus mirati su argomenti specifici indirizzati anche a singole unità di personale.

Art. 30 - Attività di sensibilizzazione

L'IRCCS promuove al suo interno anche attività di sensibilizzazione che possano consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.
In tale ottica una delle iniziative di sensibilizzazione sono costituite da attività informative rivolte non solo al personale IRCCS ma anche coloro che hanno rapporti, a vario titolo con l'Istituto.
Oltre a specifiche attività formative finalizzate al continuo aggiornamento del personale autorizzato al trattamento dei dati personali, come previsto dall'art. 29 del presente Regolamento, l'IRCCS, al fine di garantire la conoscenza capillare delle disposizioni contenute nel Regolamento UE e nel presente documento, ha previsto un'area, all'interno del proprio portale web, accessibile dalla Home Page del sito, dedicata al tema della protezione dei dati personali contenente, oltre al presente documento, la normativa di riferimento, la modulistica da usare nello svolgimento delle attività istituzionali e ogni altra documentazione di supporto.
Inoltre, ad ogni nuova Unità di Personale viene consegnata una specifica comunicazione con i riferimenti

per l'acquisizione e la consultazione del presente Regolamento. Il dipendente, acquisita tale comunicazione, si impegna a scaricarne copia, prendere visione ed attenersi alle prescrizioni IRCCS in materia di protezione dei dati personali.

CAPO IV Area Amministrativa

Art. 31 - Il trattamento dei dati del personale

L'IRCCS tratta i dati, anche di natura particolare o giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo, incluso i trattamenti effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, la definizione dello stato giuridico, del trattamento economico, degli obblighi retributivi, fiscali e contabili del personale in servizio o in quiescenza.

L'IRCCS adotta le massime cautele nel trattamento di informazioni personali dei dipendenti idonee a rivelare lo stato di salute, le abitudini sessuali, l'origine razziale ed etnica, le convinzioni politiche o d'altro genere. Il trattamento dei dati particolari del dipendente deve avvenire secondo i principi di necessità e di indispensabilità.

La pubblicazione delle graduatorie per la selezione di personale o per la concessione di benefici economici, agevolazioni o contributi, deve essere effettuata dopo avere verificato che le informazioni ivi contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute. Non sono ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché ogni altra condizione idonea a rivelare informazioni di natura sensibile.

L'IRCCS gestisce il di trattamento dei dati personali dei lavoratori relativi al rapporto di lavoro in ambito pubblico, nel rispetto di quanto previsto dalla legislazione vigente e dai Provvedimenti e dalle Linee Guida del Garante per la protezione dei dati personali.

Art. 32 - Reclutamento del personale

Nel caso di reclutamento di nuove unità di personale l'IRCCS provvede a corredare la documentazione necessaria con un'informazione trasparente sulle modalità di trattamento dei dati dei candidati. Viene richiesto uno specifico consenso al trattamento e viene chiesto di fornire due curricula: il primo completo di tutti dati identificativi, eventualmente anche di natura particolare (appartenenza a categorie protette) o giudiziari, del soggetto partecipante al bando di selezione; un secondo contenente solo il nome e cognome

dell'interessato ed epurato di qualunque altro dato (residenza, numero di telefono, codice fiscale ecc...). Quest'ultimo sarà quello che verrà sottoposto a pubblicazione se previsto dalla legge.

Art. 33 – Pubblicazione graduatorie

Le graduatorie saranno pubblicate come previsto dal regime di pubblicità delle singole norme di settore ma nel rispetto del principio di pertinenza e non eccedenza. Non possono formare oggetto di pubblicazione: i recapiti degli interessati (utenze di telefonia fissa o mobile, posta elettronica), il codice fiscale, l'indicatore ISEE, il numero di figli disabili, i risultati di test psico attitudinali o i titoli di studio, né quelli concernenti le condizioni di salute degli interessati (ivi compresi i riferimenti a condizioni di invalidità). Sono, ove possibile, inserite in area riservata ad accesso selezionato.

Art. 34 – Pubblicazione albo pretorio on line ed Amministrazione trasparente

Salvo diversa disposizione di legge, i documenti da pubblicare sul sito istituzionale per finalità di trasparenza e/o pubblicità non devono consentire l'identificabilità dei soggetti cui i dati si riferiscono quando contengono dati non necessari alla divulgazione, dati di natura particolare, dati giudiziari o di minori. Per quanto sopra, ciascun Ufficio competente alla redazione e conservazione del documento verifica caso per caso, con l'ausilio ove necessario del Responsabile della Protezione dei Dati, e seguendo le istruzioni impartite dalla Direzione Generale, la presenza di eventuali dati da oscurare o rendere anonimi o da pseudonimizzare (quali a titolo esemplificativo ma non esaustivo, numeri telefonici private, indirizzo di residenza, carta d'identità, patologie, dati del casellario giudiziale), procedendo in tal caso a curare la omissione dei medesimi dati dal contenuto del documento, prima di trasmettere il medesimo per la relativa pubblicazione al soggetto addetto a tale attività.
Per assicurare comunque la completezza delle deliberazioni, i dati personali da escludere dalla pubblicazione sono contenuti nell'originale integrale del documento a disposizione degli uffici competenti e del personale appositamente autorizzato.

Art. 35 - Il diritto di accesso e il diritto alla riservatezza

L'IRCCS, in osservanza delle disposizioni vigenti in materia di riservatezza e trasparenza, valuta, anche con riguardo ad altre regolamentazioni specifiche, caso per caso la possibilità da parte di terzi di accedere a documenti contenenti dati personali e particolari. L'accesso ai dati idonei a rivelare lo stato di salute o la vita sessuale o l'orientamento sessuale di un terzo (crfr. art. 60 Codice Privacy) è ammesso solo quando il diritto da tutelare, tramite istanza di accesso, è di rango almeno pari al diritto alla riservatezza, ovvero consiste in un diritto della personalità o altro diritto o libertà

fondamentale ed inviolabile, quale ad esempio il diritto alla difesa, sempre che le informazioni richieste siano pertinenti e non eccedenti le finalità per cui è richiesto l'accesso. Fatto salvo quanto sopra, I presupposti, le modalità, i limiti per il diritto di accesso a documenti amministrativi contenenti dati personali e la relativa tutela giurisdizionale, restano disciplinati dalla Legge 7/8/1990, n.241 ed s.m.i. e dalle altre disposizioni di legge in materia. I presupposti, le modalità ed i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal Decreto Lgs 14 marzo 2013, n.33, come modificato dal D. lgs n.97/2016 e s.m.i.

Art. 36 – Trattamento dei dati su supporto cartacei

Il personale autorizzato al trattamento dei dati dovrà avere cura di trattare i dati su supporto cartaceo secondo le modalità e con gli accorgimenti di seguito illustrati:
a) identificare gli eventuali soggetti ammessi ad accedere ai Dati Personali detenuti su supporto cartaceo al di fuori dell'orario di lavoro;

b) identificare e comunicare al Titolare gli archivi presso l'unità, dove riporre i documenti contenenti i Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili, (armadi, stanze, casseforti, ecc.);

d) verificare, previa consultazione con il Titolare, la corretta esecuzione delle procedure di distruzione dei documenti quando non più necessari o quando richiesto dall'interessato.

e) trattare i Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili, e/o Giudiziari secondo il principio di necessità, ovvero unicamente per lo scopo per cui sono stati raccolti;

f) non diffondere o comunicare i Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili e/o Giudiziari a soggetti non autorizzati al trattamento;

g) non lasciare incustoditi documenti contenenti Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili e/o Dati Giudiziari durante e dopo l'orario di lavoro;

h) non lasciare in luoghi accessibili al pubblico i documenti contenenti Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili e/o Giudiziari;

i) riporre i documenti negli archivi quando non più operativamente necessari;

l) limitare allo stretto necessario l'effettuazione di copie e/o la trasmissione all'esterno dei suddetti documenti.

La riproduzione di documenti contenenti "categorie particolari di dati personali", c.d. Dati Sensibili, e/o Giudiziari su supporti non informatici (ad esempio fotocopie) è vietata se non assolutamente indispensabile per l'esecuzione del Contratto. La riproduzione deve essere sottoposta alla medesima disciplina dei documenti originali.

Art. 37 - Consultazione dei documenti cartacei

La consultazione dei documenti contenenti Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili, e/o Dati Giudiziari, deve avvenire esclusivamente da parte degli Autorizzati, solo quando operativamente necessario e quando possibile in loco.
L'Autorizzato può effettuare la consultazione di tali documenti fuori orario di lavoro solo se preventivamente autorizzato dal Responsabile, identificato e registrato dalla vigilanza.
Distruzione dei documenti cartacei
In relazione alle previsioni di cui all'art. 5, paragrafo e), e 89 del Regolamento (UE) 2016/679, che prevedono la conservazione dei dati personali per un tempo ben definito, i documenti che non devono essere conservati per legge, devono essere distrutti al termine della loro utilizzazione.
La distruzione dei documenti nei limiti consentiti dalla legge, deve essere effettuata quando è espressamente richiesto dall'interessato e/o quando comunicato dal Titolare ovvero dall'Autorizzato/Responsabile interno della propria area di competenza e deve essere da loro formalizzata ed autorizzata in relazione alla titolarità dei dati contenuti nel documento in esame.

La distruzione legittima dei documenti cartacei contenenti dati personali deve essere effettuata, attraverso opportuni strumenti (distruggidocumenti) e comunque in modo da rendere impossibile la ricostruzione del documento.

CAPO V Area Sanitaria

Art. 38 - Ordine di precedenza e di chiamata

Nell'erogare prestazioni sanitarie o espletando adempimenti amministrativi che richiedono un periodo di attesa (ad es. in caso di analisi cliniche, prestazioni specialistiche ecc...) i pazienti non devono essere chiamati per nome, ma devono essere adottate soluzioni che prevedano un ordine di precedenza e di chiamata degli Interessati, che prescinda dalla loro individuazione nominativa, attribuendo loro un codice numerico o alfanumerico fornito al momento della prenotazione o dell'accettazione). Quando la prestazione medica può essere pregiudicata in termini di tempestività o efficacia dalla chiamata non nominativa dell'Interessato (ad es. nel caso di paziente disabile) possono essere utilizzati altri accorgimenti adeguati ed equivalenti come ad esempio il contatto diretto con il paziente

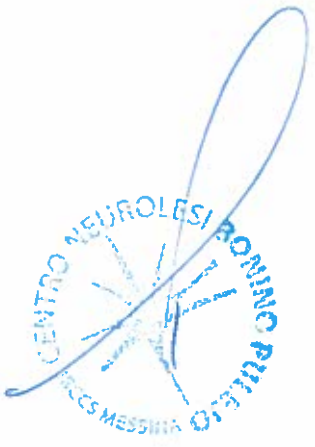
Art. 39 - Liste di pazienti

Deve essere assolutamente evitata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta. Non devono essere resi visibili ad estranei documenti sulle condizioni cliniche dell'Interessato, come le cartelle infermieristiche poste vicino al letto di degenza o liste di pazienti in attesa di intervento effettuato o ancora da erogare (es. liste di degenti che devono subire un intervento chirurgico).

Art. 40 - Liste di attesa

Le richieste di ricovero sono soggette a rivalutazione temporale:

- Se provenienti da struttura per Acuti, sono rivalutate dopo 15 giorni;
- Se provenienti da visite ambulatoriali, sono rivalutate dopo 90 giorni;
- Le istanze che superano i 12 mesi, sono eliminate dalle liste d'attesa.



Dopo il secondo rifiuto della richiesta di ricovero o per altre comprovate indisponibilità, la Commissione Ricoveri può procedere all'esclusione dell'istanza.
Le liste d'attesa sono pubblicate on line sul sito istituzionale che riporta la posizione, il codice, la richiesta e il punteggio. Il codice viene inviato via mail all'indirizzo fornito per iscritto dall'interessato.

Art. 41 – Colloqui nelle prestazioni sanitarie

Durante lo svolgimento di colloqui, specie con il personale sanitario (ad es. in occasione di prescrizioni o di certificazioni mediche), devono essere adottate idonee cautele per evitare che le informazioni sulla salute dell'Interessato possano essere conosciute da terzi. Le stesse cautele devono essere adottate in occasione della raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali (es. locali per più prestazioni) o dalle modalità utilizzate.

Art. 42 - Richiesta notizie su prestazioni di pronto soccorso

La notizia o la conferma di una prestazione, della presenza o del passaggio di una persona al pronto soccorso, richieste anche per via telefonica, possono essere fornite correttamente ai soli terzi legittimati, quali possono essere familiari, parenti o conviventi, nominativamente indicati dall'Interessato, nell'acquisizione del consenso al trattamento dei dati, se non impossibilitato e valutate le diverse circostanze del caso. Il personale Autorizzato deve accertare l'identità dei terzi legittimati a ricevere la predetta notizia o conferma, avvalendosi anche di elementi desunti dall'Interessato. Le informazioni che possono essere fornite riguardano solo la circostanza che è in atto o si è svolta una prestazione di pronto soccorso e non anche informazioni più dettagliate sullo stato di salute dell'Interessato. L'Interessato – se cosciente e capace – deve essere preventivamente informato (ad. es. in fase di accettazione) e posto in condizione di fornire indicazioni circa i soggetti che possono essere informati della prestazione di pronto soccorso. Occorre altresì rispettare eventuali sue indicazioni specifiche o contrarie.

Art. 43 - Ricovero dei pazienti in reparto

Possono essere fornite informazioni sulla presenza dei degenti nelle UU.OO. ai soli terzi legittimati e nominativamente indicati dall'Interessato. Il paziente cosciente e capace deve essere, all'atto del ricovero, informato e posto in condizione di fornire indicazioni circa i soggetti che possono venire a conoscenza del ricovero e della U.O. di degenza (utilizzando la modulistica predisposta dall'Azienda). Deve essere altresì rispettata l'eventuale sua richiesta che la presenza nella struttura sanitaria non sia resa nota nemmeno ai terzi legittimati. Quando sia stato manifestato dall'Interessato un consenso specifico e distinto al riguardo, possono comunque essere fornite informazioni sul suo stato di salute ai soggetti dallo stesso nominativamente indicati.

Art. 44 - Regole di comportamento di pazienti e Visitatori

In tutti gli ambienti dell'A.O.U. è **vietato fumare**. L'inosservanza comporta una sanzione amministrativa.

I pazienti non possono assumere **farmaci** non prescritti dal medico ospedaliero perché possono essere nocivi per possibili effetti collaterali con le terapie in corso.
E' preferibile evitare la presenza di **bambini** in ospedale, al di sotto dei 12 anni
I Visitatori potranno entrare in reparto soltanto durante gli **orari** di visita che possono subire delle variazioni in base all'organizzazione interna di ogni singolo reparto. Tuttavia possono essere consentite deroghe solo se approvate dal Dirigente Medico e per una motivazione specifica. Gli utenti sono tenuti a rispettare comunque gli orari del reparto così come le eventuali limitazioni di accesso indicate dal personale.
Per l'utilizzo (con cuffie / auricolari) di apparecchi **radio-TV** nelle camere di degenza occorre rivolgersi al personale di reparto.
Ove non espressamente vietato, l'uso del **cellulare** va limitato nel rispetto della quiete altrui (dopo le ore 21 occorre disattivare le suonerie). Prima di utilizzare il cellulare, per evitare eventuali interferenze radio con le apparecchiature mediche occorre sempre, anche in assenza degli appositi cartelli di divieto, chiedere il permesso al personale di reparto. **E' vietato fare fotografie, riprese audio video sia per i ricoverati che per i visitatori.**
E' vietato depositare oggetti o bottiglie sui **davanzali** interni o esterni delle finestre per non esporre i passanti a rischio di infortunio.
Il personale non è responsabile degli oggetti di valore, gioielli, somme di denaro. E' opportuno non lasciarli **incustoditi**.
Il personale sanitario è deputato a fare rispettare le norme di comportamento per il buon andamento del reparto e per il benessere dell'utenza.

Art. 45 - Cartelle cliniche elettroniche

La Cartella Clinica Elettronica è uno strumento di lavoro che permette attraverso il diario giornaliero, la sistematica raccolta cronologica, logica e obiettiva delle informazioni sul paziente continuamente aggiornate, necessarie a formulare diagnosi più efficienti ed efficaci e alla progettazione del piano assistenziale definito per obiettivi da raggiungere.

Secondo quanto dispone il Codice della Privacy 196/2003 come modificato dal D. Lgs. 101/2018, eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:
a) di esercitare o difendere un diritto in sede giudiziaria ai sensi dell'articolo 9, paragrafo 2, lettera *f*), del Regolamento, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale;
b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale.

Capo VI Area Ricerca Scientifica

Art. 46 – Ricerca medica, biomedica ed epidemiologica

Secondo quanto dispone il Codice della Privacy 196/2003 come modificato dal D. Lgs 101/2018, il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera *j*), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.
Il trattamento ulteriore dei dati da parte di terzi a fini di ricerca scientifica o statistici, a norma dell' art. 110 bis del Codice della Privacy novellato, non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e provati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento.

CAPO VII Area Informatica

Art. 47 – Adozione misure di sicurezza

Secondo quanto dispone l'art. 32 del GDPR 2016/679 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 varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Art. 48 – Utilizzo hardware e software

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.
Il custode delle parole chiave riservate, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.
Non è consentito installare autonomamente programmi provenienti dall'esterno salvo autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici* dell'IRCCS Bonino Pulejo. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*.
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici aziendali.*
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici aziendali* nel caso in cui vengano rilevati virus.

Art. 49 – Utilizzo della rete

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il *Responsabile dei sistemi informatici aziendali* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

Art. 50 – Rilascio credenziali di autenticazione

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal *Responsabile dei sistemi informatici aziendali.*
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Responsabile dei sistemi informatici aziendali.*
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici aziendali*, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Responsabile dei sistemi informatici aziendali.*

Art. 51 – Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici aziendali* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Art. 52 – Uso della posta elettronica

La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).
È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Art. 53 – Uso della Rete Internet e dei relativi servizi

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile dei sistemi informatici aziendali.*
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

CAPO VIII Disposizioni finale

Art. 54 - Responsabilità in caso di violazione delle disposizioni in materia di privacy

Il mancato rispetto delle disposizioni in materia di protezione dei dati personali è punito con le sanzioni di natura amministrativa e di natura penale previste dagli art. da 166 a 172 del D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018 nonché con sanzioni di natura disciplinare per violazione di regolamenti dell'IRCCS.

Il Responsabile del trattamento risponde per danno causato dal trattamento se non ha adempiuto agli obblighi previsti dal presente regolamento a lui specificatamente attribuiti o ha agito in modo difforme o contrario rispetto alle istruzioni impartite dal titolare del trattamento.

Il titolare e il responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo a loro imputabile.

Art. 55 – Abrogazione regolamento precedente

Il presente regolamento entra in vigore ad intervenuta esecutività della relativa delibera di approvazione, in sostituzione di ogni precedente regolamentazione interna nella medesima materia e viene pubblicato nel sito istituzionale: www.irccsme.it nella sezione "Amministrazione Trasparente" e nella sezione "Privacy e Protezione dei dati".

Art. 56 - Rinvio a disposizioni di legge

Per quanto non espressamente previsto nel presente regolamento, si fa rinvio al Regolamento Europeo 2016/679 del 27.04.2016 ed al D. Lgs. n. 196/03, modificato dal D. Lgs n.101/2018, ai provvedimenti specifici del Garante per la protezione dei dati personali ed alle disposizioni normative correlate.

Il Commissario Straordinario
Dott. Vincenzo Barone