Regione Sicilia
Azienda Ospedaliera Papardo
C.da Papardo - 98158 Messina - centralino 090-3991
C.F. e Partita IVA 03051880833

REGOLAMENTO

Per la protezione dei dati personali

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

ALLEGATO ALLA DELIBERA N. 271 DEL 13.03.2019

PREMESSA

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.

La normativa vigente sulla quale si fonda il Regolamento sulla protezione dei dati dell'Azienda Ospedaliera Papardo di Messina riguarda:

- Il Regolamento Europeo 2016/679 anche detto GDPR
- Il D.Lgs. 196/2003 "Codice della Privacy " come modificato dal D. Lgs. 101/2018;
- D .Lgs. 82/2005 "Codice Amministrazione digitale" successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217 per promuovere e rendere effettivi i diritti di cittadinanza digitale;
- Legge 241/1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e ss.mm.;
- D.Lgs. 33/2013 "Trasparenza della pubblica amministrazione" come modificato dal D. Lgs. 25/05/2016 n° 97;
- Provvedimenti e linee guida del Garante della Privacy.

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.

Art. 1 - Oggetto

Il presente Regolamento disciplina il trattamento dei dati personali effettuato dall'AO PAPARDO, 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 – Finalità del trattamento

Il trattamento dei dati personali è effettuato dall'AO Papardo, 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'AO Papardo; per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 4 Attività di sensibilizzazione

L'AO Papardo promuove al suo interno 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 formative ed informative rivolte non solo al personale dell'AO Papardo 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, l'AO Papardo, al fine di garantire la conoscenza capillare delle disposizioni contenute nel Regolamento UE e nel presente documento, ha 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 ed 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 dell'AO Papardo in materia di protezione dei dati personali.

Art.5 - 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.6 - 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. 7 - Dati trattati

L'AO PAPARDO tratta dati personali, particolari e giudiziari 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'AO PAPARDO;
- soggetti che per motivi di studio, tirocinio, stage o volontariato frequentano le strutture dell'AO PAPARDO ed effettuano trattamento di dati personali, quali specializzandi, allievi tirocinanti, volontari, ecc;
- clienti e imprese che intrattengono rapporti con l'AO PAPARDO 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'AO PAPARDO 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. 8 - Il trattamento dei dati del personale

L'AO PAPARDO 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'AO PAPARDO 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'AO PAPARDO 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. 9 - 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 dai soggetti autorizzati. 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. 10 - Informazione trasparente

L'AO PAPARDO, 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'AO PAPARDO 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'AO PAPARDO e presso l'apposita sezione del portale web www.aopapardo.it

Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente dell'AO PAPARDO, 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'AO PAPARDO 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.

Art. 11 - 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'AO PAPARDO 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'AO PAPARDO organizza modalità atte a facilitare l'espressione del consenso da parte dell'interessato, secondo le modalità e le forme previste dalla normativa 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 anche sul sito web dell'AO PAPARDO, previa consegna o 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'AO PAPARDO.

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'AO PAPARDO fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, l'AO PAPARDO 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'AO PAPARDO 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 - Limiti alla conservazione dei dati personali

L'AO PAPARDO 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'AO PAPARDO.

Art. 19 - Titolare del trattamento

L'AO PAPARDO, 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. 28. 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. 20 - 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'AO PAPARDO con apposita deliberazione 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 Autorizzato 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. 7 e 8 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.

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 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 Protezione dei dati e ne indirizza le attività. 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. 21 - 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/Autorizzato.

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'AO PAPARDO in attività che comportano il trattamento di dati personali per conto dell'AO PAPARDO.

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. 22 - Responsabile 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 **protocollo@pec-aopapardo.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'AO PAPARDO.

Art 23 - Amministratore di sistema

L'AO PAPARDO 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'AO PAPARDO 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".

Art. 24 - Il Responsabile dei Sistemi Informatici Aziendali

Il Responsabile dei Sistemi Informatici aziendali è Responsabile della Sicurezza informatica per la privacy per le procedure informatiche installate sui sistemi centrali e sui sistemi periferici ad essi collegati, nonché sui server delle reti di personal computer.

A lui spetta il compito di programmare ed attuare un livello di sicurezza per la protezione dei dati commisurato allo stato dell'arte e alla natura dei dati trattati in ciascuna struttura (dati identificativi della persona – dati amministrativi - dati sanitari) ed in particolare deve:

• procedere ad una ricognizione periodica delle misure di protezione esistenti e alla valutazione

dei rischi;

• governare il processo di archiviazione ed aggiornamento delle password.

Art. 25 - 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. 26 - 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'AO PAPARDO, 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

1. La valutazione contiene almeno:
2. una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dall' AO PAPARDO;
3. una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
4. una valutazione dei rischi per i diritti e le libertà degli interessati;
5. 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.
6. Se necessario l'AO PAPARDO 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.
7. 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'AO PAPARDO prima di procedere al trattamento consulta il Garante della Privacy, avvalendosi del supporto del DPO.

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'AO PAPARDO 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'AO PAPARDO possono trattare dati personali solo se autorizzati e istruiti in tal senso dall'AO PAPARDO 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'AO PAPARDO 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'AO PAPARDO, 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'AO PAPARDO: www.aopapardo.it

Art. 28 - Misure organizzative per la tutela della riservatezza

Presso tutti i presidi dell'AO PAPARDO 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. 29 - Pubblicità degli atti e diritto alla riservatezza

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. 30 - Il diritto di accesso e il diritto alla riservatezza

L'AO PAPARDO, 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. 31 - Violazione dei dati personali

Ogni SATD è tenuto ad informare senza ingiustificato ritardo l'AO PAPARDO 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'AO PAPARDO avvia le necessarie procedure e, avvalendosi della collaborazione dei Responsabili del trattamento, accerta l'effettivo stato dell'arte.
L'AO PAPARDO 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.

Art. 32 - Istruzioni di carattere generale per tutti gli Autorizzati al trattamento

Gli Autorizzati al trattamento dei dati devono:

□ **Mantenere il segreto** sulle informazioni di cui si venga a conoscenza nello svolgimento della propria attività lavorativa e professionale e nel corso delle operazioni del trattamento, 22 evitando di comunicare le informazioni a terzi. Segreto professionale: tutto il personale del ruolo sanitario, tecnico, professionale e amministrativo, sia del comparto che della dirigenza, e chiunque presti la propria attività lavorativa, anche in veste di consulente, libero professionista o volontario, nei servizi o strutture dell'Azienda è tenuto al segreto professionale ossia a non rivelare e/o agevolare in qualsiasi modo, senza giusta causa, la conoscenza delle notizie, dei dati o banche di dati di cui, in ragione e in occasione del proprio stato o ufficio, sia venuto a conoscenza. Si ricorda che l'eventuale violazione di tale obbligo può comportare l'applicazione di sanzioni di natura deontologica e disciplinare, nonché una responsabilità di natura amministrativa, civile e penale, secondo quanto previsto dal Codice;

□ **fornire l'informativa** all'Interessato o alla persona presso cui si raccolgono i dati, con le modalità determinate dall'Autorizzato/Responsabile interno della struttura di appartenenza e utilizzando la modulistica predisposta dall'Azienda;

□ **raccogliere il consenso dell'Interessato** al trattamento dei dati idonei a rivelare lo stato di salute, ogniqualvolta si erogano prestazioni finalizzate alla tutela della salute (prevenzione, diagnosi, cura e riabilitazione), con le modalità e la modulistica definite dall'Azienda;

□ **procedere alla raccolta dei dati personali** con la massima cura verificando l'esattezza degli stessi, nonché la pertinenza e la non eccedenza rispetto alle finalità da perseguire;

□ **comunicare i dati personali** di natura comune a terzi, solamente se espressamente previsto dalla legge;

□ **comunicare i dati particolari** solo a soggetti determinati e preventivamente e nominativamente individuati dall'Interessato (con le modalità e la modulistica definite dall'Azienda) o solo ove sia espressamente previsto dalla legge;

□ **non diffondere dati idonei a rivelare lo stato di salute** Per diffusione si intende "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". Sarà cura, quindi, dei soggetti che redigono gli atti oggetto di pubblicazione di far sì che si rispetti il divieto considerato. A titolo meramente esemplificativo, si suggerisce la necessità di predisporre la copia degli atti deliberativi da pubblicare, in una forma in cui vi sia il testo della stessa corredato da allegati (questi ultimi, contenenti i dati sanitari, non dovranno essere oggetto di pubblicazione, ma dovranno rimanere agli atti, conservati secondo quanto previsto dalla legge, e a disposizione di coloro che abbiano la legittimazione all'esercizio del diritto di accesso, secondo quanto

previsto dalla legge 241/90, novellata);

Art. 33 Tutela della dignità dell'Interessato

La tutela della dignità personale deve essere sempre garantita nei confronti di tutti i soggetti cui viene erogata una prestazione sanitaria con particolare riguardo a fasce deboli quali disabili, fisici e psichici, minori e anziani, nonché - per effetto di specifici obblighi di legge o di regolamento – a pazienti sieropositivi o affetti da infezione da Hiv, a pazienti sottoposti a trattamenti medici invasivi o per i quali è doverosa una particolare attenzione (es. interruzione di gravidanza e persone offese da atti di violenza sessuale).

Nelle UU.OO. di rianimazione dove si possono visitare i degenti solo attraverso vetrate o videoterminali devono essere adottati accorgimenti, anche provvisori (ad esempio mediante paraventi), che delimitino le visibilità dell'Interessato, durante l'orario di visita, ai soli familiari e conoscenti.

Art. 34 Riservatezza nei colloqui e 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. 35 - 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 e nominativamente indicati dall'Interessato, quali possono essere familiari, parenti o conviventi, 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 (utilizzando la modulistica predisposta dall'Azienda per comunicazione dello stato di salute). Occorre altresì rispettare eventuali sue indicazioni specifiche o contrarie.

Art. 36 - Dislocazione dei pazienti nelle UU.OO.

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 e allegata al presente manuale);

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. 37 - Distanza di cortesia

Nel rispetto dei canoni di confidenzialità e della riservatezza dell'Interessato, tutti i punti accettazione devono essere muniti di strumenti idonei a garantire la distanza di cortesia per gli utenti sia per operazioni amministrative allo sportello (prenotazioni), sia al momento dell'acquisizione di informazioni sullo stato di salute, sensibilizzando anche gli utenti con cartelli, segnali ed inviti. Tali strumenti possono essere sostituiti, a titolo meramente esemplificativo, da una riga gialla di segnalazione posta a terra e da un cartello che indichi il rispetto della distanza di cortesia, o qualunque altro sistema, che garantisca il medesimo risultato.

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) 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) o sui carrelli delle terapie farmacologiche.

Art. 40 - Correlazione fra paziente e U.O. o struttura

Devono essere adottate specifiche procedure per prevenire che soggetti estranei possano evincere in modo esplicito l'esistenza di uno stato di salute del paziente attraverso la semplice correlazione tra la sua identità e l'indicazione della struttura o della U.O. presso cui si è recato o è stato ricoverato. Tali cautele devono essere adottate anche per le eventuali certificazioni richieste per fini amministrativi non correlati a quelli di cura come ad esempio le certificazioni chieste per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi ad una procedura concorsuale.

Analoghe garanzie, infine, devono essere adottate nel caso di spedizione di plichi postali evitando che sugli stessi appaiano informazioni idonee a rivelare l'esistenza di uno stato di salute dell'Interessato come l'indicazione della tipologia del contenuto del plico o della U.O. mittente.

Art. 41 - Comunicazione di dati all'Interessato riguardanti il suo stato di salute

La comunicazione al paziente di informazioni sul suo stato di salute deve essere effettuata solo da un medico o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga

rapporti diretti con il paziente stesso (ad es. un infermiere autorizzato dal Direttore di Struttura quale Autorizzato/Responsabile interno).

Si possono dare informazioni sullo stato di salute a soggetti diversi dall'Interessato quando questi abbia manifestato uno specifico consenso (utilizzare la modulistica predisposta dall'Azienda per comunicazione dello stato di salute). In caso di impossibilità fisica o incapacità dell'Interessato o, valutato il caso, tale consenso può essere dato da un familiare o da persone legittimate a farlo (da chi esercita legalmente la potestà (per le informazioni relative ai nascituri il consenso è prestato dalla gestante), ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'Interessato).Nel caso specifico della comunicazione all'Interessato degli esiti di esami clinici effettuati, l'intermediazione può essere soddisfatta accompagnando un giudizio scritto con la disponibilità del medico a fornire ulteriori indicazioni a richiesta.

Art. 42 - Ritiro delle analisi

I referti diagnostici, i risultati delle analisi e i certificati rilasciati dai laboratori di analisi o dagli altri organismi sanitari possono essere ritirati anche da persone diverse dai diretti Interessati purchè munite di delega scritta e con consegna in busta chiusa.

Art. 43 - Istruzioni specifiche per tutti gli Autorizzati al trattamento dei dati per il corretto uso e la sicurezza degli strumenti aziendali. Utilizzo del personal computer in dotazione

Il trattamento di dati personali (e ancor più di dati sensibili e giudiziari) attraverso l'uso di personal computer o video terminali richiede le seguenti misure di sicurezza per la privacy:

1) il trattamento di dati personali con personal computer è consentito soltanto ai Soggetti Autorizzati dotati di password di accesso personale che consente il superamento di una procedura di autenticazione che consiste in un codice per l'identificazione associato ad una parola chiave riservata (password) conosciuta solamente dagli Autorizzati;

2) utilizzare il personal computer in dotazione, esclusivamente per ragioni di lavoro e per conto dell'Azienda;

3) assicurarsi che quando si sta lavorando al computer nessuno possa conoscere i dati che si stanno digitando o i file su cui si sta lavorando, ponendo attenzione a posizionare il monitor in modo da evitare che persone estranee possano visualizzare la schermata di lavoro;

4) durante una sessione personale di trattamento e/o di lavoro il personal computer non deve essere lasciato incustodito ed accessibile ai non Autorizzati;

5) in ogni caso di allontanamento, anche temporaneo, dalla postazione di lavoro, per sicurezza per la privacy, disconnettere la sessione di lavoro bloccando l'operatività del computer (es. logout, CTRL+ALT+CANC), da riattivare solo attraverso l'inserimento del Codice di accesso/password personali;

6) in alternativa al punto 5) utilizzare lo screen-saver protetto con password in modo da evitare che in caso di prolungata assenza i dati possano essere accessibili a soggetti estranei;

7) spegnere il computer in caso di assenza prolungata dal posto di lavoro. Un computer accesso è maggiormente attaccabile in quanto raggiungibile tramite la rete o direttamente sulla postazione di lavoro.

Lasciare un computer acceso aumenta il rischio che un'interruzione dell'energia elettrica possa causare un danno;

8) quando vengono lanciate stampe di documenti, l'Autorizzato del trattamento deve presidiare l'operazione e prelevare immediatamente i documenti stampati onde evitare la consultazione degli stessi da parte di persone non autorizzate;

9) è vietato modificare in alcun modo la postazione di lavoro (es. installazione di modem o schede di rete o quant'altro) senza formale autorizzazione ed il presidio di un tecnico dell'ufficio informatico aziendale;

10) è vietato modificare le impostazioni di sicurezza per la privacy del PC (es. SW antivirus, impostazioni del browser, ecc.) senza formale autorizzazione ed il presidio di un tecnico dell'ufficio informatico aziendale;

11) non lasciare mai incustodito un notebook aziendale in ufficio o in viaggio (particolare attenzione deve essere riposta quando si viaggia sui mezzi pubblici);

12) durante le missioni di lavoro, portare il notebook come bagaglio a mano, evitando di trasportare in borsa i codici identificativi e le parole chiave di sicurezza per la privacy, nonché i supporti di memorizzazione con le copie di back-up;

13) non lasciare esposto in automobile in sosta il notebook aziendale.

Il Responsabile della sicurezza informatica qualora rilevi, nell'esercizio della sua funzione, l'utilizzo improprio da parte del dipendente del personal computer in dotazione, relativamente ai punti da 2 a 10 sopracitati, dovrà predisporre apposita relazione in merito e proporre al Direttore della S.C., ove presta servizio il predetto dipendente, che nei confronti del predetto dipendente venga attivata il consequenziale provvedimento disciplinare; il Direttore della S.C. in questione dovrà attivare tempestivamente il suindicato provvedimento.

Art. 44 - Username e Password

1) Il responsabile SIA assegna a ciascun Autorizzato ad operare su una postazione di lavoro uno username come chiave di accesso riconducibile ad una singola persona. Le chiavi di accesso possono coincidere per lo stesso utente su diversi sistemi.

2) L'utente a cui viene assegnato per la prima volta uno username, riceve anche una password temporanea che dovrà modificare alla prima connessione. La password è il codice che rende "personale" la chiave, garantendone la riservatezza. La robustezza e segretezza delle password sono meccanismi fondamentali per la protezione di buona parte dei sistemi. Pertanto, la scelta della propria password deve rispondere ai seguenti **requisiti minimi**:

a) **Lunghezza**: dovrà avere una lunghezza minima di 8 caratteri alfanumerici (lettere e numeri) ed almeno due caratteri speciali e lettere maiuscole e minuscole;

b) **Complessità**: non deve contenere riferimenti agevolmente riconducibili al proprietario della stessa (es. data di nascita, nome dei figli, nome utente, etc.) e deve essere generata preferibilmente senza un significato compiuto;

c) **Ripetitività**: non potrà essere riutilizzata. Alla scadenza dovrà sempre essere impostata una password

diversa da quelle impostate precedentemente;

d) **Scadenza**: la password assegnata deve essere prontamente sostituita al primo utilizzo e deve essere modificata con cadenza trimestrale;

3) la password deve essere comunicata per iscritto, in busta chiusa, dopo averne controfirmato i lembi, al Direttore della U.O. di appartenenza che, in qualità di Autorizzato, potrà aprire la busta ed utilizzare la password (previa apposita verbalizzazione) nei casi di necessità previsti in assenza dal servizio dell'Autorizzato;

4) all'atto della consegna della busta ciascun Autorizzato dovrà firmare un apposito verbale di consegna datato;

5) le password non utilizzate da almeno sei mesi verranno disattivate;

6) le password sono disattivate anche in caso di perdita della qualità che consente all'Autorizzato l'accesso (es. trasferimento, pensionamento, etc.);

7) il proprio codice di accesso/password deve essere custodito con la massima attenzione e segretezza e non deve essere divulgato o comunicato a terzi o lasciarne una trascrizione in luoghi accessibili a terzi;

8) il possessore della password è responsabile di ogni utilizzo indebito o non consentito della stessa;

9) fare attenzione a non essere "osservati" durante la digitazione di una password o qualunque codice di accesso;

10) non permettere l'uso della propria password a soggetti terzi, per cui solamente in caso di necessità (intervento di assistenza o di manutenzione) richiedere la finalità della richiesta ed accertarsi dell'identità del soggetto che richiede la comunicazione della vostra password.

Art. 45 - Supporti di memorizzazione

1) se possibile, archiviare sempre i dati e tutti i documenti elettronici (word, excel, access...) utilizzati per effettuare trattamenti di dati personali sul server centrale di rete ed eliminarli dall'hard disk del personal computer in dotazione. Questa misura di sicurezza per la privacy permette di proteggere con maggiore efficacia l'accesso ai dati da persone non autorizzate al trattamento 2) non salvare informazioni di natura particolare su supporti rimovibili (es. CD, DVD, pen drive, ecc.) salvo che non ne sia consentita la crittografia degli stessi. In ogni caso devono essere conservati in strutture chiuse a chiave e mai lasciati incustoditi;

4) Se non più utilizzati, i supporti rimovibili contenenti dati particolari o giudiziari devono essere distrutti;

5) nel caso di utilizzo di pen drive, per la memorizzazione di dati, fare attenzione a disinserire le chiavi dalle porte USB seguendo la procedura di disconnessione sicura;

6) i supporti rimovibili non vanno mai ceduti a terzi; nel caso in cui sono consegnate a terzi per trasferire dati, assicurarsi che sui supporti di memorizzazione siano presenti solamente i dati necessari da trasferire, ovvero effettuare personalmente l'operazione di trasferimento, evitando di consegnare i supporti stessi a terzi, che potrebbero copiare le informazioni personali memorizzate;

7) eliminare documenti cartacei e dai supporti di memorizzazione in maniera sicura, evitando di gettarli

nel cestino della spazzatura, senza averli previamente resi inutilizzabili utilizzando gli idonei distruggi documenti o averli distrutti in maniera appropriata dal supporto di memorizzazione informatico;

8) accertarsi che le informazioni non più utili vengano cancellate in modo sicuro dai supporti di dati e non conservare inutilmente messaggi di posta elettronica.

Art. 46 - Virus

1) i virus possono alterare o addirittura distruggere i dati e i programmi;

2) i virus diffusi in internet sono spesso camuffati da programmi di utilità o di intrattenimento;

3) ogni computer è protetto da idonei strumenti per il rischio di attività di virus informatici;

4) lo strumento di protezione (di norma software antivirus) è abilitato;

5) è vietato disattivare, senza autorizzazione, il software antivirus;

6) la posta elettronica viene filtrata in entrata da un apposito prodotto antivirus che pulisce gli eventuali allegati contenenti virus. Evitare di aprire messaggi provenienti da mittenti sconosciuti o sospetti e cancellarli immediatamente;

7) nel caso di utilizzo di supporti di memorizzazione esterni, controllare sempre che i file memorizzati non siano infettati da virus attraverso la scansione del supporto;

8) controllare periodicamente la presenza di virus sul personal computer in dotazione mediante la scansione dell'intero sistema.

Art. 47 - Software

Alle misure di sicurezza informatiche operate centralmente si richiede l'applicazione delle seguenti misure di sicurezza per postazioni locali:

1) sul computer in dotazione può essere utilizzato solamente il software fornito dall'azienda;

2) non si possono installare software e applicazioni sul personal computer in dotazione senza una specifica autorizzazione da parte dell'Azienda ed il presidio di un tecnico del servizio informatico aziendale;

3) non creare e non utilizzare software senza licenza d'uso, È consentito unicamente l'utilizzo di software ufficialmente acquisiti ed inventariati dall'azienda.

4) provvedere al salvataggio (backup) degli archivi e documenti elettronici esistenti localmente sul personal computer con frequenza almeno settimanale;

5) adottare, relativamente all'accesso ai locali ove sono conservati i dati ed effettuati i trattamenti, misure di sicurezza per la privacy analoghe a quelle descritte per i trattamenti effettuati su supporto cartaceo (es. impedire l'accesso ai personal computer chiudendo a chiave le stanze).

Art. 48 - Divieto di valutazioni automatizzate

E' vietato adottare un atto amministrativo contenente una valutazione del comportamento umano fondandolo unicamente su un trattamento automatizzato di dati personali, volto a definire il profilo o la personalità dell'Interessato. Pertanto in tutti i casi in cui l'Azienda si avvale di procedure informatizzate

per monitorare, ad esempio, la presenza in servizio (timbrature), l'adozione di provvedimenti deve essere assunta valutando anche le altre circostanze.

Art. 49 - Posta elettronica

1) Ogni utente deve utilizzare la posta elettronica messa a disposizione dall'azienda esclusivamente per necessità di lavoro;

2) i messaggi di posta elettronica ricevuti o spediti con l'indirizzo di posta elettronica aziendale non costituiscono corrispondenza personale del dipendente o collaboratore aziendali, per cui possono essere conosciuti da terzi per esigenze operative e istituzionali;

3) le informazioni trasmesse – molto spesso - possono/devono essere condivise per cui deve essere salvaguardata l'integrità e la confidenzialità dei messaggi e dei contenuti;

4) si deve evitare di rispondere ai c.d. "invii a catena" degli utenti di internet o ai messaggi di solidarietà che richiedono di inviare un'e-mail a un certo indirizzo o a un certo numero di utenti, poiché possono essere veicoli di diffusione di virus informatici ovvero sistemi per la raccolta di indirizzi di posta elettronica, per l'invio di comunicazioni commerciali non desiderate o di posta cd. spazzatura;

5) evitare di rispondere a messaggi promozionali o di spamming;

6) evitare di trasmettere per posta elettronica contenuti che possano essere considerati di contenuto molesto/osceno, razzista, pedo-pornografico o illegale, nonché aventi natura ingiuriosa o diffamatoria;

7) evitare di registrare il proprio indirizzo di posta elettronica su siti web sospetti c/o mailing list non direttamente correlate all'attività istituzionale aziendale.

Art. 50 - Internet

1) Internet deve essere utilizzato esclusivamente per ragioni di lavoro;

2) non si deve utilizzare l'accesso ad internet per fini personali, che esulano dall'attività lavorativa;

3) è vietato accedere a siti web contenenti materiale pedo-pornografico, materiale fraudolento illegale,

materiale blasfemo/molesto/osceno;

4) è, altresì, vietato tentare di violare o aggirare i sistemi di controllo o di protezione dell'uso di internet e della posta elettronica installati e utilizzati dall'azienda, nel rispetto del diritto alla riservatezza dei dipendenti;

5) è, infine, vietato installare e/o utilizzare in modo fraudolento strumenti concepiti per compromettere la sicurezza per la privacy dei sistemi (ad esempio strumenti di "password cracking", "network probing",...).

Art. 51 - Rete di comunicazione

1) è vietato allacciare alla rete di comunicazione aziendale strumenti elettronici che non siano stati forniti dall'Azienda;

2) il computer in dotazione non deve possedere o disporre di altri collegamenti esterni diretti;

3) è vietato installare mezzi di comunicazione propri (come per esempio modem);

4) utilizzare esclusivamente le installazioni messe a disposizione dall'azienda ovvero quelle che siano oggetto di specifica autorizzazione;

5) non usare mai il proprio user-id e la propria password per accedere a sistemi esterni;

6) ricorrere, eventualmente, a sistemi esterni solamente per finalità istituzionali e di lavoro.

Art. 52 - Utilizzo di telefono e fax

1) In generale, è opportuno non fornire indicazioni relative allo stato di salute degli utenti via telefono, se non si è certi dell'identità dell'interlocutore che sta chiamando;

2) verificare comunque che l'Interessato abbia autorizzato la comunicazione dei propri dati a terzi;

3) in alcuni casi, specie per chiamate di natura istituzionale (da altre strutture ospedaliere, autorità giudiziaria, soggetti pubblici), si consiglia di farsi lasciare dal chiamante il proprio nominativo ed il numero di telefono; si provvederà a ricontattare l'ente chiamante, chiedendo della persona che ha lasciato il proprio nominativo, previa verifica dell'indispensabilità dei dati richiesti rispetto alla finalità dell'utilizzo dichiarato e della previsione normativa o dell'autorizzazione dell'Interessato alla comunicazione dei propri dati;

4) nel caso in cui si debba procedere alla comunicazione di dati particolari tra unità diverse utilizzando il fax, è opportuno che lo strumento sia collocato in un'area protetta e presidiata e che gli Autorizzati prestino attenzione alle fasi di invio (verifica della corretta digitazione del numero del destinatario, inserimento di formula di riservatezza) e di ricevimento della documentazione contenente dati personali particolari e giudiziari;

5) nel caso in cui si debbano comunicare ad un ente o soggetto esterni dati sensibili utilizzando il fax, in occasione del primo rapporto con l'ente, si deve richiedere, prima dell'invio della documentazione, di indicare il numero di un fax, localizzato in luogo protetto e non accessibile al pubblico, al quale inviare la documentazione;

6) il riscontro alla richiesta di cui al punto precedente, avrà come effetto l'autorizzazione all'Azienda ad inviare esclusivamente al numero dichiarato la documentazione considerata. Ogni operatore Autorizzato del trattamento deve conservare copia della comunicazione di elezione del numero di fax, indicato per la ricezione di fax riservati.

Art. 53 - Utilizzo della stampante

1) La stampa di documentazione contenente dati personali, particolari e giudiziari deve avvenire ad opere degli Autorizzati a trattare tali dati;

2) ritirare tempestivamente la documentazione dalla stampante utilizzata;

3) il riutilizzo di fogli recanti una stampa su una sola facciata, per esigenze di risparmio e di sensibilità ambientale, deve riguardare esclusivamente supporti nella elusiva disponibilità dell'Autorizzato ed essere utilizzati nell'ambito delle proprie mansioni, evitando di far conoscere a terzi non autorizzati il contenuto dei documenti;

4) i fogli contenenti dati personali e sensibili non più utilizzati e per i quali non è necessaria la conservazione, prima di essere conferiti nella raccolta differenziata, devono essere trattati in modo da

rendere non intelligibili a terzi – usando eventualmente un dispositivo distruggi documenti – dati personali ivi contenuti.

Art. 54 - Utilizzo della fotocopiatrice

la fotoriproduzione di documentazione cartacea, contenente dati personali e, in particolare, dati particolari e giudiziari deve avvenire ad opera dell'Autorizzato autorizzato al trattamento dati.

Art. 55 - istruzioni per Autorizzati al trattamento dei dati per il corretto trattamento dei dati su supporto cartaceo

Il trattamento dei dati su supporti cartacei è uno degli aspetti maggiormente delicati in materia di sicurezza e riservatezza e pertanto richiede alcuni accorgimenti:

1) i documenti contenenti dati personali di natura sensibile devono essere custoditi in stanze o locali, o armadi o carrelli chiusi a chiave e le chiavi devono essere custodite da personale autorizzato (accesso selezionato) e va redatto dal Direttore della U.O. di appartenenza un registro ed un verbale di consegna delle chiavi; il personale Autorizzato del trattamento deve verificare che detti locali o armadi contenenti i documenti siano chiusi a chiave;

2) quando le cartelle cliniche o altra documentazione contenente dati idonei a rivelare lo stato di salute sono affidati agli Autorizzati per lo svolgimento dei relativi compiti, oppure devono essere trasferite da una struttura o da un ufficio presso altro luogo (esempio archivio di deposito) è necessario che i medesimi atti e documenti siano controllati e custoditi dagli Autorizzati e che questi utilizzino ogni cautela per la protezione della riservatezza al fine di impedire che ad essi accedano persone prive di autorizzazione, fino alla restituzione, cioè al termine delle operazioni affidate;

3) si consiglia di inserire la documentazione in busta chiusa o in raccoglitori sigillati sui quali apporre la propria firma per garantirne l'integrità;

4) evitare di scrivere dati personali di natura sensibile su lavagne o altri supporti che possano essere visionati da persone non autorizzate;

5) le cartelle e i fascicoli di lavoro devono essere tenuti sulla propria scrivania facendo attenzione che i dati eventualmente riportati sul frontespizio non siano visibili a persone non autorizzate (es. utenti del servizio);

6) nel caso di assenza, anche momentanea, dalla propria stanza, non lasciare incustoditi fascicoli, cartelle e documenti cartacei contenenti dati di natura sensibile. Si consiglia di chiudere a chiave la propria stanza, qualora rimanga incustodita senza personale all'interno, ovvero di riporre la documentazione dentro un armadio chiuso a chiave.

Art. 56 - Sicurezza degli archivi cartacei

- l'accesso agli archivi, sia operativi che remoti, contenenti dati sensibili o giudiziari, deve essere controllato e permesso unicamente agli Incaricati del trattamento e la protezione dei dati deve essere incentrata alla sicurezza per la privacy degli archivi stessi;

- va redatto, un elenco del personale Autorizzato che detiene le chiavi di detti archivi;

□ l'accesso di persone non autorizzate (es. pazienti/utenti) deve essere vietato ai locali dove i documenti sono presenti senza il presidio di un Autorizzato; l'accesso agli archivi aziendali deve essere controllato e devono essere identificati e registrati i soggetti che vi sono ammessi.

□ quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

□ i documenti contenenti dati particolari o giudiziari devono essere utilizzati dagli Autorizzati del trattamento solo per il tempo necessario allo svolgimento dei relativi compiti e poi riposti negli archivi;

□ gli Autorizzati devono custodire i documenti in maniera che ad essi non accedano persone prive di autorizzazione (es. mai lasciare incustoditi i documenti durante il loro trattamento);

□ custodire le fotocopie (autorizzate) con le stesse modalità degli originali;

□ la consegna dei documenti (es. referti) deve prevedere l'identificazione dell'Interessato o di un suo delegato e sarà eseguita in busta chiusa.

□ i trasferimenti di documenti tra Strutture interne deve prevedere l'utilizzo di buste sigillate o altre precauzioni che impediscano la consultazione degli stessi da parte di persone non autorizzate;

□ tutti i documenti non più necessari devono essere resi inutilizzabili, distrutti, resi illeggibili prima di essere cestinati (è necessario fare ricorso ai distruggi documenti: carta, CD, DVD, Pen Drive).

Art. 57 - Attività di verifica e controllo

L'AO PAPARDO definisce apposite modalità per lo svolgimento di attività di verifica e controllo, anche periodico, del rispetto delle misure di legge e delle ulteriori disposizioni AO PAPARDO 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 Autorizzato sotto il coordinamento del DPO.

Art. 58 - 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 161 a 172 del D. Lgs. 196/2003 e s.m.i. nonché con sanzioni di natura disciplinare per violazione di regolamenti AO PAPARDO.
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. 59 - Norma finale

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