Azienda Ospedaliera Universitaria
Policlinico Paolo Giaccone
di Palermo

Linee guida sul sistema di protezione dati in AOUP

Sommario

Premessa

L'Aazienda Ospedaliero Universitaria Policlinico – "Paolo Giaccone" (d'ora innanzi AOUP), con il presente documento, dà attuazione a quanto disposto con il Regolamento UE 2016/679 (d'ora innanzi GDPR - General Data Privacy Regulation) relativo alla protezione dei dati personali delle persone fisiche (interessati), fornendo indicazioni per la creazione, all'interno dell'AOUP, di un sistema di gestione della privacy basata sul principio di accountability (trasparenza).

Glossario dei termini

1. **«archivio»**: qualsiasi insieme strutturato di dati personali (digitale o cartaceo) accessibile secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
2. **«cartella clinica elettronica - CCE»**: è formata da dati personali, dati sanitari, dati genetici, dati biometrici e dati relativi alla sfera sessuale del paziente;
3. **«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;
4. **«dati personali»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile (l'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;
5. **«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;
6. **«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;
7. **«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;
8. **«destinatario»**: la persona fisica o giuridica che riceve comunicazione di dati personali di interessati. 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;
9. **«dossier sanitario»**: è un documento elettronico che raccoglie dati sanitari relativi al paziente;
10. **«diritto di accesso»:** diritto dell'interessato a richiedere al responsabile la conferma dell'esistenza o meno dei trattamenti di dati che lo riguardano e la comunicazione dei dati, nonché la copia, aggiornamento, rettifica, integrazione dei suoi dati personali;

11. **«diritto di opposizione»:** diritto dell'interessato ad avversare e far bloccare (blocking), per ragioni legittime, il trattamento di dati che lo riguardano, chiedendone, eventualmente, la cancellazione (wiping);
12. **«DPO»:** Data Protection Officer o RPD (Responsabile della Protezione dei Dati), di cui all'art. 37 del GDPR, esterno o interno all'organizzazione, nominato dal Titolare del Trattamento per supportarlo nei vari adempimenti di legge relativamente alla privacy;
13. **«fascicolo sanitario elettronico - FSE»**: insieme di dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito;
14. **«limitazione di trattamento»**: è il contrassegno su dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
15. **«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;
16. **«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;
17. **«referto on line»**: è la relazione scritta, in modalità informatica, rilasciata dal medico sullo stato clinico del paziente, dopo un esame clinico o strumentale;
18. **«responsabile del trattamento»**: la persona fisica o giuridica, esterna all'organizzazione rappresentata dal Titolare, che tratta i dati personali per conto del Titolare e da quest'ultimo è formalmente nominata;
19. **«soggetto designato quale responsabile interno del trattamento»**: la persona fisica, interna all'organizzazione rappresentata dal Titolare con un ruolo di responsabilità apicale[1], autorizzata formalmente dal Titolare al trattamento dei dati personali;
20. **«soggetto designato quale incaricato del trattamento»**: la persona fisica, interna o esterna all'organizzazione, formalmente autorizzata al trattamento dei dati personali dal Titolare dell'organizzazione (se interna all'organizzazione) o dal "Responsabile del trattamento" previamente designato dal Titolare;
21. **«soggetto designato quale incaricato AdS[2]»**: la persona fisica, interna o esterna all'organizzazione, autorizzata al trattamento dei dati personali dal Titolare dell'organizzazione (se interna all'organizzazione) o dal "Responsabile del trattamento" previamente designato;

[1] Nel nostro caso: Direttore di Dipartimento Assistenziale, UOC – Unità Operativa Complessa, UOSD - Unità Operativa Semplice Dipartimentale, UdS – Unità di Staff, medico competente, …

[2] AdS – Amministratore di Sistema con competenze, singole o complessive, sulla connessione in rete, sulla sicurezza informatica, sui database, sulle applicazioni e/o sui di sistemi operativi

22. **«terzo»**: la persona fisica o giuridica diversa dall'interessato, dal Titolare, dal "Responsabile del trattamento", dai "Soggetti designati al trattamento" dal Titolare o del "Responsabile del trattamento";
23. **«titolare del trattamento»**: la persona fisica o giuridica che determina le finalità e i mezzi del trattamento di dati personali;
24. **«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;
25. **«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.

Art. 1 - Oggetto ed ambito di applicazione

Il presente documento disciplina le modalità con cui l'AOUP tutela la persona in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal GDPR (recepito con D.Lgs. 101/2018) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
Scopo del presente documento è garantire che i dati personali siano trattati all'interno dell'AOUP in modo lecito, corretto e trasparente nei confronti dell'interessato nonché secondo i principi di limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, di cui all'articolo 5 del GDPR.
La protezione delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale riconosciuto dalla Unione Europea e a tal fine l'AOUP mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente alla normativa vigente, tenuto conto della relativa natura, ambito di applicazione, contesto e finalità di trattamento, e possibile rischio di lesione dei diritti e delle libertà degli interessati.

Art. 2 - Sensibilizzazione

L'AOUP promuove al suo interno ogni iniziativa di sensibilizzazione che possa 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 è costituita dall'attività formativa ed informativa rivolta al personale Aziendale ed a tutti coloro che hanno rapporti con l'AOUP.
Oltre a specifiche attività formative finalizzate al continuo aggiornamento dei responsabili e dei soggetti autorizzati al trattamento dei dati personali, l'AOUP, al fine di garantire la conoscenza capillare delle disposizioni contenute nel GDPR e nel presente documento, allestisce una pagina del proprio portale web dedicata al tema della protezione dei dati personali contenente, oltre al presente documento, l'informativa sul trattamento dei dati personali, la modulistica da usare nello svolgimento delle attività istituzionali ed ogni altra documentazione di riferimento e di supporto.
Inoltre, ad ogni dipendente di nuova assunzione 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 scaricare copia, prendere visione ed attenersi alle prescrizioni Aziendali in materia di protezione dei dati personali.

Art. 3 - Principi applicabili al trattamento dei dati personali

I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento UE a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

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

Art. 4 - Liceità del trattamento

Il trattamento dei dati personali è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni (art. 6 del GDPR):

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

Il trattamento delle categorie particolari di dati personali di cui all'articolo 9 del Regolamento (UE) 2016/679 (dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi

alla salute o alla vita sessuale o all'orientamento sessuale della persona) è consentito qualora si verifichi uno dei casi riportati al paragrafo 2 del medesimo articolo:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche,
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
e) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
f) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
g) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale
h) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
i) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Art. 5 - Dati trattati

L'AOUP può trattare dati personali e sensibili 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'AOUP;

- soggetti che per motivi di studio, tirocinio, stage o volontariato frequentano le strutture dell'AOUP ed effettuano trattamento di dati personali, quali specializzandi, allievi tirocinanti, borsisti, volontari, ecc;
- imprese che intrattengono rapporti con l'AOUP per la fornitura 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'AOUP nelle forme e nei limiti di quanto previsto dalla vigente normativa sono raccolti:

- prioritariamente con l'interessato o con 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. 6 - Le finalità del trattamento dei dati personali

Il trattamento dei dati personali è effettuato dall'AOUP, in quanto soggetto pubblico, ed è consentito solo per lo svolgimento delle funzioni istituzionali assegnate e, pertanto, per le seguenti finalità:

- svolgimento dei compiti del Servizio Sanitario Nazionale annoverati tra le finalità di rilevante interesse pubblico ed espletamento delle funzioni istituzionali previste dalle normative vigenti;
- 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 Hospital o altre modalità, volte alla tutela della salute e dell'incolumità fisica degli utenti, di terzi e della collettività;
- svolgimento di funzioni di didattica, formazione e ricerca scientifica, statistica ed epidemiologica, quali quelle del Registro Tumori, finalizzate alla tutela della salute;
- tutela della sicurezza e della salute dei lavoratori e sorveglianza igienico-sanitaria delle proprie strutture;
- medicina legale e gestione del contenzioso;
- gestione delle proprie risorse umane, tecnologiche, strumentali e patrimoniali in quanto soggetto Aziendale e operatore economico qualificato.

Nei casi e con i limiti previsti dalle normative settoriali vigenti vengono effettuati trattamenti di dati personali e sensibili per la rilevazione delle malattie mentali, delle malattie infettive e diffusive, della sieropositività, a fini di indagini epidemiologiche, a fini di trapianto di organi e tessuti, ai fini della tenuta del Registro Tumori, a fini di campagne di screening, ai fini del monitoraggio della spesa sanitaria.
I dati personali di tipo sensibile sono trattati qualora siano essenziali e necessari allo svolgimento delle attività istituzionali assegnate all'AOUP e nel caso in cui tali attività non possano essere adempiute mediante il trattamento di dati anonimi o di dati personali di diversa natura.
L'AOUP assicura il diritto all'anonimato dell'interessato o l'adozione di misure capaci di garantire un maggior grado di tutela della riservatezza nel trattamento dei suoi dati specificatamente previsti dalle normative vigenti.

Il trattamento dei dati personali per fini di ricerca viene effettuato con il consenso dell'interessato o, negli altri casi previsti dalla normativa vigente, previa erogazione di apposita informativa ed adozione di apposite ed adeguate misure di sicurezza.
I risultati della ricerca pubblicati o comunque resi noti non possono in alcun caso contenere dati personali che rendano identificabili i soggetti ai quali si riferiscono.

Art. 7 - Il trattamento dei dati del personale

L'AOUP tratta i dati, anche di natura sensibile 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'AOUP 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 sensibili 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'AOUP applica quanto previsto dalla normativa vigente per la protezione dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

Art. 8 - Le operazioni di trattamento

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

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

- la comunicazione, ovvero la trasmissione dei dati a uno o più soggetti determinati, in qualunque forma, anche mediante messa a disposizione o consultazione; la comunicazione dei dati avviene solo nei casi previsti da norme di legge o regolamento;
- la diffusione, ovvero il dare conoscenza dei dati personali a soggetti indeterminati (es. pubblicazione nell'albo pretorio, ecc.);
- la limitazione, cioè il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- la cancellazione;
- la distruzione.

Le operazioni di trattamento possono essere effettuate solo dal titolare, dai responsabili e dagli incaricati del trattamento. Non è consentito il trattamento da parte di persone non autorizzate.
Il responsabile della protezione dei dati provvede, in collaborazione con i responsabili del trattamento, al censimento e all'aggiornamento di tutti i trattamenti di dati personali effettuati.
È compito del responsabile del trattamento dei dati effettuare la valutazione periodica della non eccedenza dei dati trattati.

Art. 9 - 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'AOUP 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.

Art. 10 - Informazione trasparente

Il del trattamento dei dati AOUP 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'AOUP a tal riguardo predispone specifiche informative sul trattamento dei dati personali che riportano le informazioni previste dalla vigente normativa relativamente a (art. 13 e 14 Reg. UE):

a) l'identità e i dati di contatto del titolare del trattamento e del Responsabile della Protezione dei Dati;
b) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
c) gli eventuali destinatari cui possono essere comunicati i dati;
d) il periodo di conservazione dei dati personali 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 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) qualora la liceità del trattamento dei dati sia basata sul preventivo rilascio di consenso al trattamento, il diritto di revocarlo in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
g) il diritto di proporre reclamo all'Autorità Garante Privacy;
h) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione di tali dati;
i) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
j) nel caso in cui i dati personali non siano stati ottenuti presso l'interessato, la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

L'informativa all'interessato viene fornita per iscritto, anche per estratto, tramite materiale informativo reso disponibile in luoghi comuni dell'AOUP e presso l'apposita sezione del portale web dell'AOUP.
Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente dell'AOUP, 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'AOUP 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 - Il consenso al trattamento dei dati

Nel trattamento dei dati personali o sensibili, effettuati per il perseguimento di finalità di tutela dell'incolumità fisica e della salute dell'interessato, l'AOUP organizza modalità atte a facilitare l'espressione

del consenso da parte dell'interessato, secondo le modalità e le forme previste dal c.d. "Codice Privacy" aggiornato con D.Lgs. 101/2018 che recepisce gli aggiornamenti del GDPR.
In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, stato di necessità o situazione di emergenza sanitaria, il consenso può intervenire senza ritardo, successivamente alla prestazione, da parte di chi esercita legalmente la potestà o da parte di terzi legittimati.
Il consenso deve essere reso, da parte dell'interessato, attraverso la compilazione di un apposito modello disponibile sul sito web dell'AOUP, previa consegna e presa d'atto della nota 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'AOUP.

Art. 12 - 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. 5 del GDPR):

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'AOUP fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, l'AOUP 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. 13 - 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. 14 - 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. 15 - Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano e l'AOUP 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 riguarda, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

Art. 16 - 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. 17 - Comunicazione di dati all'interessato

I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato oltre che mediante consegna diretta dei dati allo stesso anche attraverso modalità telematiche nei casi e nei modi previsti dalla specifica normativa e su consenso specifico dell'interessato.
La documentazione sanitaria che viene consegnata in busta chiusa può essere ritirata dall'interessato o da altra persona diversa da questo delegata, salvo il caso dei documenti relativi a dati regolati da normative speciali che prevedono il ritiro diretto dell'interessato.

Art. 18 - Il registro delle attività di trattamento dei dati personali

L'AOUP 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 Responsabili del trattamento, 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 dai responsabili del trattamento.
Il Registro è tenuto in forma scritta, anche in formato elettronico e, su richiesta, viene messo a disposizione dell'Autorità Garante della Privacy.

Art. 19 - La valutazione di 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'AOUP, 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 valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dall'AOUP;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati; e
d) 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 GDPR,

tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Se necessario l'AOUP 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.

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'AOUP prima di procedere al trattamento consulta il Garante della Privacy avvalendosi del DPO.

Art. 20 - Il titolare del trattamento dei dati personali

Il titolare del trattamento dei dati personali è 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.

Il Titolare del trattamento dei dati personali ai sensi e per gli effetti del Regolamento è l'**AOUP**, rappresentata dal Direttore Generale / Commissario Straordinario, in qualità di rappresentante legale della stessa, con sede legale in Via del Vespro, 129 - 90127 Palermo.

Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, quali la pseudonimizzazione e la cifratura dei dati personali (se possibile), la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati.

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

In aggiunta a quanto sopra, il Titolare del trattamento:

- nomina con proprio atto i responsabili del trattamento dei dati personali impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, all'esercizio dei diritti dell'interessato di cui al Capo III del citato GDPR;
- tiene un registro delle attività di trattamento svolte sotto la propria responsabilità;
- in caso di violazione dei dati personali provvede alla notifica all'autorità di controllo senza ingiustificato ritardo secondo le modalità e i contenuti di cui all'art. 33 del GDPR;
- svolge, nei casi previsti dal GDPR, una valutazione d'impatto sulla protezione dei dati consultandosi con il responsabile della protezione dei dati (DPO);
- procede, qualora necessario, alla consultazione preventiva di cui all'art. 36 del GDPR.

Art. 21 – soggetto designato quale Responsabile interno del trattamento

Per "soggetto designato quale Responsabile interno trattamento" si intende la persona fisica con ruolo organizzativo AOUP apicale che tratta dati personali.
In considerazione della complessità e della molteplicità delle funzioni istituzionali svolte dall'AOUP, il Titolare del trattamento designa soggetti individuati quali Responsabili interni unicamente i soggetti che ricoprono posizioni apicali assistenziali/amministrative tra cui:

- i Direttori dei dipartimenti assistenziali;
- i titolari di UOC (Unità Operativa Complessa);
- i titolari di UOSD (Unità Operativa Semplice Dipartimentale);
- i titolari di UdS (Unità di Staff);
- i medici competenti.

Il soggetto designato quale responsabile interno del trattamento comunica al Titolare i soggetti designati quali Incaricati al trattamento dati per la relativa autorizzazione formale sempre da parte del Titolare; tra questi dovranno essere autorizzati gli AdS.
Il titolare del trattamento informa ciascun responsabile del trattamento dei dati delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti. I trattamenti da parte di un responsabile interno del trattamento sono disciplinati da atto scritto che vincola il responsabile del trattamento al titolare del trattamento e che stabilisce la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.
Il soggetto designato quale responsabile interno del trattamento inoltre:

- tratta i dati personali solo su istruzione documentata del titolare del trattamento;
- comunica, in forma scritta, al Titolare i nomi dei soggetti da designare quali incaricati al trattamento dei dati personali, nell'ambito della propria struttura (Dipartimento, Unità, …) per i trattamenti di dati di propria competenza, e si assicura che gli stessi si siano impegnati a mantenere la riservatezza di tali dati o abbiano un adeguato obbligo legale di riservatezza;
- osserva le disposizioni Aziendali in materia di tutela dei dati personali, nonché le specifiche istruzioni impartite dal titolare del trattamento, e mette in atto tutte le misure di sicurezza indicate dall'AOUP e le ulteriori misure tecniche ed organizzative per garantire ai dati oggetto di trattamento un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, natura, oggetto, contesto e finalità del trattamento, rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- cura la diffusione delle norme, delle linee guida e di ogni altra disposizione impartita dall'AOUP fra i soggetti autorizzati al trattamento dei dati personali;
- adotta ulteriori istruzioni interne e indicazioni di comportamento per il personale, i pazienti, gli studenti, i tirocinanti e i visitatori;
- verifica l'esattezza, l'aggiornamento, la pertinenza e la congruità dei dati, in rapporto all'attività svolta;
- effettua, limitatamente all'ambito e agli aspetti di competenza, l'analisi dei rischi che incombono sui trattamenti dei dati e nella conservazione dei medesimi;

- verifica periodicamente il corretto trattamento dei dati personali da parte dei soggetti incaricati del trattamento;
- segnala al DPO l'inizio o la cessazione di trattamenti di dati personali e della cancellazione di dati personali, al fine di permettere l'aggiornamento del registro delle attività di trattamento;
- segnala tempestivamente al DPO e al Titolare del trattamento ogni violazione dei dati personali;
- svolge ogni altra funzione specificatamente riportata nell'art. 28 del GDPR, cui si rimanda per integrale riferimento, tra cui, in particolare:
    - assiste il Titolare del trattamento, nella misura in cui ciò sia possibile e tenendo conto della natura del trattamento e delle informazioni a sua disposizione, al fine di soddisfarne l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato e garantire il rispetto degli obblighi di legge;
    - mette a disposizione del Titolare del trattamento le informazioni necessarie per dimostrare il rispetto degli obblighi di legge previsti dall'art. 28 del GDPR e contribuisce alle attività di controllo, revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un soggetto da questi incaricato.

Art. 22 - Responsabili (esterni) del trattamento

I soggetti esterni all'AOUP cui sono affidate attività di competenza Aziendale di qualunque natura (ad esempio: videosorveglianza, assistenza informatica, sicurezza, gestione della rete, della telefonia, …), che comportano necessariamente il trattamento di dati personali di cui l'AOUP è titolare, vengono individuati quali responsabili del trattamento qualora presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di legge e garantisca la tutela dei diritti dell'interessato.
Il Responsabile del trattamento svolge le medesime funzioni di cui al precedente art. 21 e indica al titolare i soggetti formalmente incaricati al trattamento dati (inclusi gli eventuali AdS) di propria competenza.
Le strutture interne dell'AOUP che provvedono alla stesura o validazione degli atti che disciplinano i rapporti con i soggetti esterni (contratti, convenzioni, scritture private, conferimenti, etc.), sono tenute ad inserire negli atti stessi l'indicazione che l'AOUP provvederà a designare successivamente, ma comunque prima di procedere al trattamento dei dati, il contraente quale Responsabile del trattamento dei dati personali e a impartire allo stesso specifiche disposizioni operative.

Art. 23 - Soggetti incaricati del trattamento dei dati personali

I soggetti incaricati del trattamento dei dati personali 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 e vigilano sul rispetto di tali istruzioni, anche attraverso verifiche periodiche.
Possono essere altresì incaricati 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'AOUP in attività che comportano il trattamento di dati personali per conto dell'AOUP.

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.

Art. 24 - Il Responsabile della Protezione dei Dati (DPO)

Il Responsabile della Protezione dei Dati, o Data Protection Officer (DPO), è designato dall'AOUP 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 GDPR.
L'AOUP pubblica i dati di contatto del DPO e li comunica all'Autorità Garante della Privacy in conformità alle indicazioni di tale Autorità, e si assicura che sia tempestivamente e adeguatamente coinvolto su tutte le questioni riguardanti la protezione dei dati personali.
Il Direttore Generale fornisce al DPO le risorse umane, tecnologiche, strumentali ed economiche necessarie per assolvere ai suoi compiti, accedere ai dati personali e ai trattamenti e mantenere la propria conoscenza specialistica.
Il DPO si avvale di referenti per la privacy che saranno individuati in modo capillare nell'ambito delle varie strutture dell'AOUP e si assicura della massima collaborazione della UdS "Sistema Informativo Aziendale" e di ogni altra articolazione Aziendale che gestisce le infrastrutture ICT in merito all'applicazione interna delle misure di sicurezza e di protezione dei dati personali per i trattamenti automatizzati adottati.
Il DPO attiva tutte le misure per favorire l'osservanza del presente documento e delle altre disposizioni vigenti relative alla protezione dei dati e svolge altresì i seguenti compiti:

- riferisce al Direttore Generale dell'AOUP sulle problematiche relative alla protezione dei dati personali;
- informa e fornisce consulenza al Direttore Generale, ai responsabili del trattamento, agli incaricati del trattamento dei dati personali in merito agli obblighi derivanti dalla normativa vigente in materia di protezione dei dati;
- sorveglia l'osservanza del presente documento e delle altre disposizioni vigenti relative alla protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento;

- predispone, anche su iniziativa del Direttore Generale e in stretto raccordo con i responsabili dei servizi interessati, la modulistica, linee guida, procedure, disposizioni operative, registri e policy necessari a rendere operative le indicazioni di legge e del presente documento;
- coopera e funge da punto di contatto per l'Autorità Garante della Privacy per tutte le questioni connesse al trattamento dei dati personali, consultandolo quando necessario.

Nell'eseguire i propri compiti il DPO considera debitamente i rischi inerenti al trattamento dei dati, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Art. 25 - L'AdS (Amministratore di Sistema)

Il Titolare nomina formalmente gli AdS, in seno alla propria organizzazione, su indicazione del Responsabile interno della UdS Sistema Informativo Aziendale, previa valutazione dell'esperienza, capacità e affidabilità del soggetto designato al trattamento dati il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di sicurezza sui dati relativamente alla loro riservatezza, integrità e disponibilità. La designazione sarà sempre individuale e sarà effettuata mediante apposito atto e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato; l'operatività degli AdS può abbracciare uno o più ambiti tra quelli sottoelencati:

- AdS di rete;
- AdS di database;
- AdS di sicurezza informatica;
- AdS di applicativi;
- AdS di sistemi operativi.

I "Responsabili del trattamento" in outsourcing con AOUP (Cineca, CNR, …) nomineranno a loro volta gli AdS di loro competenza.

Art. 26 - Le misure di sicurezza

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'AOUP 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'AOUP possono trattare dati personali solo se autorizzati e istruiti in tal senso dall'AOUP 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'AOUP 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'AOUP, 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.

Art. 27 - Misure organizzative per la tutela della riservatezza

Presso tutti i presidi dell'AOUP 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 sensibili 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. 28 - Pubblicità degli atti e diritto alla riservatezza

Salvo diversa disposizione di legge, i documenti contenenti dati sensibili da pubblicare all'Albo Pretorio oppure oggetto di pubblicazione per finalità di trasparenza, non devono consentire l'identificabilità dei soggetti cui i dati si riferiscono.
L'AOUP assicura che in sede di predisposizione degli atti stessi e dei relativi allegati si proceda all'oscuramento dei dati personali idonei a rivelare lo stato di salute o delle altre informazioni da cui si possa desumere, anche indirettamente, l'esistenza di patologie o di condizioni di invalidità, disabilità, handicap fisici e/o psichici.
I dati sensibili devono essere sottratti all'indicizzazione e alla rintracciabilità mediante i motori di ricerca web esterni ed al loro riutilizzo.
L'AOUP applica in materia le disposizioni contenute nel provvedimento n. 243 del Garante per la protezione dei dati personali del 15/05/2014 "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati".

Art. 29 - Il diritto di accesso e il diritto alla riservatezza

L'AOUP, 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 sensibili.

L'accesso ai dati idonei a rivelare lo stato di salute o le abitudini sessuali di un terzo 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.

Si rinvia per gli ulteriori aspetti al regolamento aziendale sul diritto di accesso.

Art. 30 - La tenuta in sicurezza dei documenti ed archivi dell'AOUP

Gli archivi che custodiscono i dati di cui è titolare del trattamento l'AOUP, cartacei o digitali, devono essere collocati in locali idonei in ossequio alle disposizioni generali in materia di sicurezza e a quelle specifiche per la protezione del patrimonio informativo Aziendale.
La documentazione archiviata, anche digitalmente, contenente i dati personali è conservata secondo le modalità e i tempi previsti dalla legge e poi sottoposta a scarto di archivio o distruzione come da vigente normativa.
I responsabili del trattamento, attenendosi alle indicazioni del Responsabile della Protezione dei Dati ed alle disposizioni e procedure Aziendali vigenti, attivano meccanismi necessari a garantire l'accesso selezionato ai dati e l'accesso controllato ai locali dove questi sono collocati mediante registrazione degli accessi ed esclusione degli stessi fuori dell'orario di servizio dell'archivio medesimo.
I supporti contenenti dati personali diversi dal cartaceo (supporti informatici, magnetici, videoregistrazioni effettuate nell'ambito dell'attività clinica, immagini iconografiche), debbono essere conservati e custoditi secondo le modalità e i termini previsti dalla normativa vigente.
Gli archivi cartacei e digitali sono oggetto di trattamento da parte del responsabile del trattamento dei dati di competenza, che deve assicurarne la riservatezza, protezione ed integrità per tutto il tempo in cui ne mantiene la disponibilità.
Relativamente agli archivi informatizzati di dati l'AOUP adotta idonee procedure di:

- salvataggio periodico degli archivi di dati personali;
- misure di contenimento dei virus/malware informatici e di protezione perimetrale da cyberattacchi alle infrastrutture ICT Aziendali;
- disaster recovery e continuità operativa;
- conservazione sostitutiva come da vigente normativa.

Art. 31 - Limiti alla conservazione dei dati personali

L'AOUP 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'AOUP
- 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'AOUP.

Art. 32 - La violazione dei dati personali

Ogni responsabile o soggetto incaricato del trattamento dei dati personali è tenuto ad informare senza ingiustificato ritardo l'AOUP 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'AOUP avvia le necessarie procedure e, avvalendosi della collaborazione dei Responsabili del trattamento, accerta l'effettivo stato dell'arte.
L'AOUP 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 DPO 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. 33 - Attività di verifica e controllo

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

Art. 34 - 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, nonché con sanzioni di natura disciplinare per violazione di regolamenti Aziendali.
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. 35 - Norma finale

Per quanto non espressamente previsto nel presente regolamento, si fa rinvio alla vigente normativa legislativa e regolamentare, ai provvedimenti specifici del Garante per la protezione dei dati personali, al GDPR e al codice privacy aggiornato con D.Lgs. 101/2018.
L'AOUP si riserva di apportare al presente regolamento le modifiche, rettifiche e/o integrazioni ritenute necessarie alla luce di eventuali innovazioni normative in materia di riservatezza e protezione dei dati personali, nonché ritenute opportune e/o necessarie dal DPO.

Informativa sul trattamento dei dati personali

(art. 13 D. Lgs. n. 196/2003 e ss.mm.ii. - art. 13 e 14 Regolamento UE 2016/679)

Gentile utente,
ai sensi del D.Lgs. n. 196/2003 – Codice in materia di protezione dei dati personali – aggiornato con D.Lgs. 101/2018 - si informa che l'AOUP (Azienda Ospedaliero Universitaria Policlinico "Paolo Giaccone") per l'erogazione delle prestazioni richieste e per tutte le attività amministrative e di legge connesse, effettua il trattamento di dati personali, tra cui quelli idonei a rivelare lo stato di salute e la vita sessuale, da Lei direttamente comunicati o eventualmente raccolti presso gli uffici dell'AOUP. Il citato Codice prevede che chi effettua trattamenti di dati personali sia tenuto ad informare l'interessato su taluni aspetti qualificanti il trattamento.

FINALITÀ DEL TRATTAMENTO

Il trattamento dei Suoi dati personali si svolge nel rispetto dei principi di correttezza, liceità e trasparenza, tutelando la riservatezza ed i diritti dell'interessato, oltreché nel rispetto delle norme sul segreto professionale e d'ufficio, per le seguenti finalità:

- **assistenziali**, allo scopo cioè di erogare prestazioni di prevenzione, diagnosi, cura e riabilitazione, sia in regime di ricovero che ambulatoriale, anche in libera professione intramuraria;
- **amministrativo/contabili** correlate all'assistenza e/o allo svolgimento dei compiti del Servizio Sanitario Nazionale quali, ad esempio: prenotazione, compilazione di documentazione sanitaria, refertazione, certificazione, archiviazione, produzione dei flussi informativi previsti dalla legge, rilascio di copia della documentazione sanitaria su richiesta degli interessati o degli aventi diritto, trapianti di organo e trasfusioni di sangue, ecc.
- **didattico-formative**, in riferimento alla possibile presenza, nel percorso assistenziale, di personale non strutturato (medici specializzandi, personale volontario o tirocinante), essendo questa AOUP ente strumentale all'Università degli Studi di Palermo.
- **ricerca scientifica o statistico-epidemiologica** finalizzata alla tutela della salute ed incolumità fisica dell'interessato, di terzi e della collettività**:** l'AOUP, ove possibile, procede a rendere i dati personali anonimi ed aggregati in modo da non consentire l'identificazione dei soggetti interessati.
- **analisi di gradimento e valutazione della qualità dei servizi,** al fine di migliorare la qualità dei servizi erogati.

L'AOUP può inoltre prevedere forme di collaborazione con altri enti sanitari anche mediante strumenti di telemedicina e teleconsulto e in tali casi l'AOUP può comunicare o trasmettere, con il consenso dell'interessato, dati e documenti sanitari per ottenere il supporto clinico necessario.
L'AOUP effettua attività di video sorveglianza all'interno delle pertinenze Aziendali per ragioni di tutela della salute e sicurezza dei degenti, dei visitatori e degli operatori nonché del patrimonio Aziendale. I sistemi di videosorveglianza sono evidenziati da apposita segnaletica e gestiti nel rispetto di quanto stabilito dal Garante per la Protezione dei dati personali.

MODALITÀ DI TRATTAMENTO DEI DATI

Tutte le operazioni di trattamento dei dati (ad esempio: raccolta, registrazione, elaborazione, conservazione, ecc.) vengono effettuate da personale debitamente istruito ed autorizzato, nel rispetto del segreto professionale e del segreto d'ufficio e in accordo con i principi di pertinenza, non eccedenza e di indispensabilità. I dati sono trattati utilizzando supporti cartacei o informatici nel rispetto delle misure di sicurezza previste dalla normativa e conservati in archivi protetti e custoditi.

COMUNICAZIONE A SOGGETTI TERZI

I dati da Lei forniti, indispensabili per l'erogazione della prestazione sanitaria richiesta e per le attività amministrative ad essa correlate, potranno essere comunicati, quando ciò sia previsto da una legge o da un regolamento o nel caso risulti comunque necessario per lo svolgimento delle funzioni istituzionali, a soggetti terzi tra cui, a titolo esemplificativo: Organi dello Stato, Regione Siciliana, enti del Servizio Sanitario Nazionale, esercenti le professioni sanitarie, soggetti esterni che svolgono specifici incarichi per conto dell'AOUP (ad esempio conservazione delle cartelle cliniche, patrocinio legale, ecc).
L'eventuale comunicazione ad altri soggetti, sia pubblici che privati, se non prevista in ottemperanza ad obblighi normativi, può essere effettuata solo previa specifica informativa ed acquisizione di distinto e autonomo consenso. Non viene effettuata alcuna diffusione di dati idonei a rivelare il Suo stato di salute, ai sensi dell'art. 22, comma 8 del Codice.
Per la tutela della riservatezza, il personale dei reparti o ambulatori è tenuto a non fornire informazioni telefoniche riguardanti le condizioni di salute delle persone assistite.

TITOLARE DEL TRATTAMENTO E RESPONSABILE DELLA PROTEZIONE DEI DATI

Titolare del trattamento dei dati da Lei forniti è l'AOUP il cui rappresentante legale è il Direttore Generale / Commissario Straordinario. Con apposito atto l'AOUP designa i responsabili del trattamento, tenuti ad osservare le istruzioni in materia di protezione dei dati personali, il cui elenco è consultabile presso l'URP ed è pubblicato sul sito web. Le operazioni di trattamento dei dati sono effettuate da incaricati nominati dal titolare e dai vari responsabili che ricevono specifiche disposizioni operative a garanzia dei diritti dell'interessato.
Per tutte le problematiche inerenti la tutela della privacy l'AOUP ha individuato il DPO (responsabile della protezione dei dati), contattabile al seguente indirizzo: dpo@policlinico.pa.it e con le altre modalità riportate nella pagina "Privacy" del sito web Aziendale www.policlinico.pa.it

DIRITTI DELL'INTERESSATO

In relazione al trattamento dei dati personali che La riguardano la vigente normativa Le riconosce la facoltà di esercitare i diritti previsti dal D.Lgs. n. 196/2003 e s.m.i. tra cui:

1. il diritto di ottenere: a) la conferma che sia o meno in corso un trattamento di dati personali che La riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle informazioni previste dalla citata normativa; b) la rettifica dei dati personali inesatti, l'integrazione di quelli incompleti; c) la cancellazione dei dati, salvo che per motivi di interesse pubblico nel settore della sanità pubblica o per altre condizioni specificatamente previste dalla vigente normativa; d) la limitazione del trattamento, nei casi previsti dalla legge; e) la portabilità dei dati, in caso di dati personali raccolti sulla base del consenso e trattati con mezzi automatizzati.
2. Il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, salvo le situazioni previste dalla normativa.
3. Il diritto di revocare il consenso in qualsiasi momento. In tal caso potrebbe non essere garantita l'erogazione della prestazione sanitaria richiesta.
4. Il diritto di proporre reclamo all'Autorità Garante per la Protezione dei dati personali.

MODALITÀ DI ESERCIZIO DEI DIRITTI

La richiesta per l'esercizio dei diritti di cui sopra deve essere presentata all'AOUP Ospedaliero-Universitaria Policlinico "P. Giaccone", titolare del trattamento, all'indirizzo della Direzione Generale in Via del Vespro, n. 129 – 90127 Palermo oppure all'indirizzo PEC protocollo.aoup@pec.policlinicogiaccone.it o alla mail privacy@policlinico.pa.it

Io sottoscritto/a ……..……..
Nato/a a ……..……prov. ……. il ……

In qualità di:

□ diretto/a interessato/a □ esercente la potestà genitoriale □ tutore/curatore/ amministratore di sostegno □ prossimo congiunto/coniuge/familiare/convivente

di ……..……
Nato/a a ……..……prov. ……. il ……

DICHIARO

di avere ricevuto e compreso il contenuto della presente informativa predisposta dal titolare del trattamento dei dati personali ai sensi dell'art. 13 del D. Lgs. n. 196/2003 e s.m.i. e degli art. 13 e 14 Regolamento UE 2016/679.

Esprimo il consenso al trattamento dei dati personali per le finalità elencate nella presente informativa:

□ Si □ No

Data …… Firma ...……