IMMEDIATAMENTE ESECUTIVA

AZIENDA OSPEDALIERA
OSPEDALI RIUNITI VILLA SOFIA - CERVELLO

DELIBERA DEL DIRETTORE GENERALE

N° 300 **DEL** 27 FEB 2020

OGGETTO: **Approvazione "Regolamento per la protezione dei dati personali".**

STRUTTURA PROPONENTE: *U.O.C. Coordinamento Strutture di Staff* **PROPOSTA N°** 46 **DEL** 26.02.2020

Il Dirigente e/o il responsabile del procedimento attestano – con la sottoscrizione del presente atto ed a seguito dell'istruttoria effettuata – la regolarità della procedura seguita, che l'atto è legittimo nella forma e nella sostanza nonché utile per il servizio pubblico.

L'ESTENSORE DEL PROVVEDIMENTO	IL RESPONSABILE DELLA PROTEZIONE DEI DATI	IL DIRETTORE U.O.C. COORD. STRUTTURE DI STAFF
P. i. Michele Ruggiano	*P. i. Michele Ruggiano*	
(firma)	*(firma)*	*(firma)*
Data: 26/2/2020	Data: 26/2/2020	Data:

Il Funzionario addetto al controllo di budget attesta – con la sottoscrizione del presente atto – che lo stesso non comporta scostamenti sfavorevoli rispetto al budget economico e, pertanto, ne attesta la copertura economica dei costi. Attesta, inoltre, il NULLA OSTA in quanto conforme alle norme sulla contabilità.

Conto Economico *(n°)*: /

Importo *(€)*: nessun onere

Sub-autorizzazione *(numero)*: /

IL FUNZIONARIO ADDETTO AL CONTROLLO DI BUDGET *Dr.* _____ Data 26/02/2020 Firma

Il Dirigente
U.O.C. Economico - Finanziario e Patrimoniale
Dott.ssa Alga Giuliana

PARERE DEL DIRETTORE AMMINISTRATIVO *Dr.ssa Rosanna Oliva*	PARERE DEL DIRETTORE SANITARIO *Dr. Aroldo Gabriele Rizzo*
☒ Favorevole ☐ Non Favorevole *(con motivazioni allegate al presente atto)*	☐ Favorevole ☐ Non Favorevole *(con motivazioni allegate al presente atto)*
Data 27.2.2020 Firma	Data 27/2/2020 Firma

Il presente provvedimento si compone di n. ____ pagine, di cui n. ____ pagine di allegati.

IL DIRETTORE GENERALE
Dr. Walter Messina

In data 27 FEB 2020 nella sede legale dell'Azienda Ospedaliera "*Ospedali Riuniti Villa Sofia – Cervello*" di Palermo, Viale Strasburgo n. 233, P.I. 05841780827

IL DIRETTORE GENERALE
Dr. Walter Messina

nominato con Decreto del Presidente della Regione Siciliana n. 198 del 4 aprile 2019, con l'intervento del Direttore Amministrativo Dr.ssa Rosanna Oliva, nominato con Delibera n. 256 del 21 giugno 2019 e del Direttore Sanitario Dr. Aroldo Gabriele Rizzo, nominato con Delibera n. 257 del 21 giugno 2019, assistito dal segretario verbalizzante Giuseppe Bartolotta, adotta la seguente deliberazione

DELIBERA DEL DIRETTORE GENERALE

U.O.C. COORDINAMENTO STRUTTURE DI STAFF
IL RESPONSABILE DELLA PROTEZIONE DEI DATI
P. i. Michele Ruggiano

VISTA la deliberazione n.181 dell'11/2/2011 con la quale questa Azienda ha adottato il regolamento aziendale sul trattamento dei dati sensibili e personali, in applicazione del D.lgs. 30/6/2003, n.196 (Codice in materia di protezione dei dati personali), che ha recepito sul territorio nazionale la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati;

ATTESO che il Parlamento europeo e il Consiglio, del 27 aprile 2016, hanno adottato il Regolamento (UE) 2016/679 (GDPR – *General Data Protection Regulation*) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati, che ha abrogato la richiamata direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;

PRESO ATTO che il testo del suddetto Regolamento (UE) 2016/679 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea del 4/5/2016 ed è divenuto definitivamente applicabile in tutti i Paesi UE a far data dal 25/5/2018;

VISTO il D.lgs. 10/8/2018, n.101, recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27/4/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*", che ha sostanzialmente integrato e modificato il citato Codice in materia di protezione dei dati personali di cui al D.lgs. 30/6/2003, n.196;

ATTESO che le norme introdotte dal Regolamento (UE) 2016/679 (GDPR) si traducono in adempimenti organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy;

RICHIAMATA la deliberazione n.1479 del 10/9/2018 con la quale questa Azienda ha designato, ai sensi dell'art.37 del citato GDPR, il Responsabile della protezione dei dati, da ultimo sostituito con deliberazione n.991 del 24/12/2019;

RICHIAMATA la deliberazione n.656 del 3/10/2019 con la quale questa Azienda ha costituito il Gruppo di lavoro per la protezione dei dati;

RICHIAMATA la deliberazione n.657 del 3/10/2019 con la quale questa Azienda ha costituito l'Ufficio per la protezione dei dati;

PRECISATO che nel contesto dell'art.26 dell'Atto Aziendale, adottato da questa Azienda con deliberazione n.631 del 30/9/2019 e successiva n.142 del 30/1/2020, è prevista la delega ai Direttori di strutture delle funzioni di Responsabile del trattamento dei dati di cui al citato GDPR, e ciò in applicazione di quanto prescritto dall'art.2-*quaterdecies* del citato D.lgs. n.196/2003 e s. m. e i.;

ATTESA l'esigenza di definire modalità organizzative, misure procedimentali e regole di dettaglio che permettano a questa Azienda di potere agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal GDPR;

VISTO lo schema di "*Regolamento per la protezione dei dati personali*" allegato al presente atto, redatto dal Responsabile della protezione dei dati proponente in conformità al

Regolamento (UE) 2016/679 (GDPR) e connesso D.lgs. 10/8/2018, n.101, nonché nel rispetto delle previsioni dell'Atto Aziendale;

PRESO ATTO che detto schema di Regolamento è stato favorevolmente esitato dal citato Gruppo di lavoro nelle apposite riunioni del 17/2/2020 e del 24/2/2020, di cui alle rispettive verbalizzazioni;

RAVVISATA l'esigenza di procedere all'approvazione del Regolamento in esame, che concorre ad implementare gli adempimenti già posti in essere per la puntuale attuazione delle varie previsioni del nuovo quadro normativo in materia di privacy introdotte dal GDPR;

PRECISATO che il nuovo Regolamento in approvazione sostituisce e annulla quello approvato con la citata deliberazione n.181 dell'11/2/2011;

ATTESO che il Responsabile del procedimento e il Responsabile della struttura proponente attestano l'assenza di conflitto di interessi, ai sensi della normativa vigente e del Codice di Comportamento;

ATTESO che il Responsabile della Struttura proponente attesta la liceità e la regolarità delle procedure poste in essere con il presente provvedimento, in quanto legittime ai sensi della normativa vigente con riferimento alla materia trattata, nonché attesta l'utilità e l'opportunità per gli obiettivi aziendali e per l'interesse pubblico;

PROPONE

Per i motivi indicati in premessa che qui si intendono integralmente riportati, di:

1) **Approvare** il "*Regolamento per la protezione dei dati personali*", allegato al presente atto per formarne parte integrante, redatto dal Responsabile della protezione dei dati proponente in conformità al Regolamento (UE) 2016/679 (GDPR) e connesso D.lgs. 10/8/2018, n.101, nonché nel rispetto delle previsioni dell'Atto Aziendale citati in premesse, come favorevolmente esitato dal Gruppo di lavoro per la protezione dei dati costituito da questa Azienda.

2) **Dare atto** che la presente deliberazione non comporta alcun onere di spesa.

3) **Procedere** alla pubblicazione del presente provvedimento sul sito aziendale – Atti e Regolamenti dell'Albo on line – per assicurare l'ampia diffusione e conoscenza dovuta al Regolamento approvato.

4) **Dare atto** che il nuovo Regolamento approvato sostituisce e annulla quello approvato con la deliberazione n.181 dell'11/2/2011 citata in premesse.

5) **Dichiarare** il presente provvedimento immediatamente esecutivo al fine di consentire a questa Azienda di porre in essere tutte le azioni necessarie per assicurare la puntuale attuazione delle varie previsioni del nuovo quadro normativo in materia di privacy introdotte dal GDPR.

6) **Incaricare** le strutture competenti dell'esecuzione del presente provvedimento.

L'ESTENSORE
DEL PROVVEDIMENTO
P. i. Michele Ruggiano

IL RESPONSABILE
DELLA PROTEZIONE DEI DATI
P. i. Michele Ruggiano

IL RESPONSABILE
DELLA STRUTTURA PROPONENTE

DELIBERA DEL DIRETTORE GENERALE

IL DIRETTORE GENERALE

IN VIRTÙ del Decreto del Presidente della Regione Siciliana n. 198 del 04 aprile 2019 di nomina del Dr. Walter Messina quale Direttore Generale dell'Azienda Ospedaliera "*Ospedali Riuniti Villa Sofia Cervello*" e della susseguente Delibera n.1 del 16 aprile 2019 di presa d'atto di detto D.P.R.S.;

VISTA la proposta di deliberazione che precede, avente ad oggetto "*Approvazione "Regolamento per la protezione dei dati personali"*";

ACQUISITI i pareri espressi dal Direttore Amministrativo Aziendale e dal Direttore Sanitario Aziendale;

RITENUTO di condividerne il contenuto;

DELIBERA

Di adottare la proposta di deliberazione per come sopra formulata dal Dirigente Responsabile della Struttura proponente e conseguentemente di:

1) **Approvare** il "*Regolamento per la protezione dei dati personali*", allegato al presente atto per formarne parte integrante, redatto dal Responsabile della protezione dei dati proponente in conformità al Regolamento (UE) 2016/679 (GDPR) e connesso D.lgs. 10/8/2018, n.101, nonché nel rispetto delle previsioni dell'Atto Aziendale citati in premesse, come favorevolmente esitato dal Gruppo di lavoro per la protezione dei dati costituito da questa Azienda.

2) **Dare atto** che la presente deliberazione non comporta alcun onere di spesa.

3) **Procedere** alla pubblicazione del presente provvedimento sul sito aziendale – Atti e Regolamenti dell'Albo on line – per assicurare l'ampia diffusione e conoscenza dovuta al Regolamento approvato.

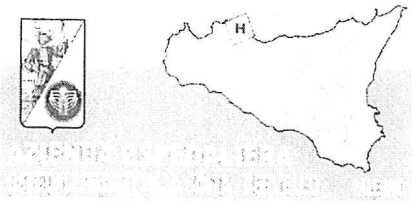
4) **Dare atto** che il nuovo Regolamento approvato sostituisce e annulla quello approvato con la deliberazione n.181 dell'11/2/2011 citata in premesse.

5) **Dichiarare** il presente provvedimento immediatamente esecutivo al fine di consentire a questa Azienda di porre in essere tutte le azioni necessarie per assicurare la puntuale attuazione delle varie previsioni del nuovo quadro normativo in materia di privacy introdotte dal GDPR.

1) **Incaricare** le strutture competenti dell'esecuzione del presente provvedimento.

IL DIRETTORE GENERALE
Dr. Walter Messina

Il Segretario Verbalizzante
(*Sig.* Giuseppe Bartolotta)



REGOLAMENTO

per la protezione dei dati personali

(Regolamento Europeo 2016/679,

D. Lgs. n.196/2003 modificato dal D. Lgs n. 101/2018)

ALLEGATO ALLA DELIBERA N._____DEL. _____

Sommario

PREMESSA

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

La principale novità introdotta dal Regolamento Europeo in materia di protezione dei dati personali 2016/679, noto anche come GDPR – General Data Protection Regulament -, consiste nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato sulla valutazione del rischio, in luogo del precedente approccio basato su adempimenti. La protezione dei dati è rimessa al Titolare del trattamento il quale, grazie al principio di responsabilizzazione ("accountability"), potrà, nei limiti e dentro i parametri delineati dal Regolamento, adottare le misure che ritiene più opportune e comprovare il conseguimento degli obiettivi che ha raggiunto nel rispetto dei principi che presiedono il trattamento dei dati personali.

Tutti coloro che a diverso titolo operano in nome e per conto dell'Azienda Ospedaliera "Ospedali Riuniti Villa Sofia Cervello di Palermo e che trattano dati personali di terzi sono formalmente designati per svolgere le attività di trattamento, ricevono istruzioni operative e formazione specifica e sono chiamati al rigoroso segreto d'ufficio. Dette designazioni hanno luogo ad avvenuta esecutività del presente Regolamento, con riferimento al personale già in servizio, ovvero, per il personale di prossima assunzione, al momento dell'immissione in servizio e, nello specifico, su espresso mandato del Titolare al momento della sottoscrizione del rispettivo contratto individuale.

Altra importante finalità da perseguire è chiarire il corretto utilizzo della strumentazione elettronica che nel tempo – senza sostituire completamente le forme tradizionali e tipiche della sanità- ha preso piede nello scambio di informazioni. Si è valutato come i principi di efficienza ed efficacia che connotano la qualità delle prestazioni sanitarie non possano e non debbano mettere a rischio le libertà fondamentali di ciascuno.

Altrettanto utile appare sottolineare come erogare servizi sanitari sia attività che "tratta dati" e lo faccia nell'accezione più ampia del termine, attraverso la loro raccolta, la registrazione degli stessi e lo studio delle loro mutazioni sia qualitative che quantitative nel corso del tempo.

La normativa vigente sulla quale si fonda il Regolamento sulla protezione dei dati dell'Azienda Ospedaliera "Ospedali Riuniti Villa Sofia Cervello di Palermo riguarda:

- Decreto Legislativo n.196 del 30/6/2003 "Codice in materia di protezione dei dati personali"
- Regolamento Europeo in materia di protezione dei dati personali 2016/679, noto anche come GDPR – General Data Protection Regulament –
- D .Lgs. n.82/2005 "Codice Amministrazione digitale" successivamente modificato e integrato prima con il Decreto Legislativo 22/8/2016 n.179 e poi con il Decreto Legislativo 13/12/2017 n.217 per promuovere e rendere effettivi i diritti di cittadinanza digitale;

- Legge n.241/1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e ss.mm.

- D.Lgs. 10/8/2018 n.101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27/4/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Art. 1 – Oggetto

Il presente Regolamento contiene disposizioni attuative del D. Lgs. n.196/03 (codice privacy) e del Regolamento UE 2016/679 (GDPR) nell'ambito delle Strutture dell'Azienda Ospedaliera "Ospedali Riuniti Villa Sofia Cervello di Palermo, di seguito denominata Azienda, con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Azienda medesima. L'Azienda adotta idonee e preventive misure di sicurezza, volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. L'Azienda adotta altresì le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi dell'art.15 del Regolamento UE 2016/679.

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 del Regolamento UE 2016/679;

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 – 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:

1. La raccolta dei dati;
2. La registrazione dei dati, ovvero il loro inserimento su supporti, automatizzati o manuali, al fine di rendere i dati disponibili per successivi trattamenti;
3. L'organizzazione dei dati, cioè il processo di lavorazione finalizzato a favorirne la fruibilità attraverso l'aggregazione, la disaggregazione, l'accorpamento, la catalogazione;

4. La conservazione dei dati;
5. L'adattamento o la modifica in relazione a variazioni o a nuove acquisizioni;
6. L'estrazione;
7. La consultazione;
8. L'uso;
9. 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;
10. La diffusione, ovvero il dare conoscenza dei dati personali a soggetti indeterminati (es. pubblicazione nell'albo pretorio, ecc)
11. La limitazione, cioè il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
12. La cancellazione;
13. La distruzione.

Le operazioni di trattamento possono essere effettuate solo dal titolare, dai responsabili o delegati e dagli incaricati o sub-delegati di cui all'art.2-*quaterdecies* del Codice della Privacy, ovvero dai responsabili di cui all'art.28, Regolamento UE 2016/679. 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 ed all'aggiornamento di tutti i trattamenti di dati personali effettuati.

E' compito del responsabile del trattamento dei dati effettuare la valutazione periodica della non eccedenza dei dati trattati.

Art. 4 – Principi applicabili al trattamento dei dati personali

Ogni trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato. Oggetto di ogni tipo di trattamento dovranno essere i soli dati essenziali per lo svolgimento delle attività istituzionali. I dati personali devono essere trattati in modo lecito e secondo correttezza e trasparenza nei confronti dell'interessato, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini compatibili con talli scopi. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per i quali sono raccolti e trattati. I dati che, anche a seguito di verifiche, risultassero eccedenti, non pertinenti o non indispensabili, non

potranno essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene. In ogni caso devono essere adottate misure tecniche tali da garantire che i dati personali o sensibili siano accessibili ai soli Incaricati di trattamento e nella misura strettamente indispensabile allo svolgimento delle mansioni di ciascuno.

Il trattamento dei dati personali è effettuato dall'Azienda, in quanto soggetto pubblico, per lo svolgimento dei compiti del Servizio Sanitario Nazionale annoverati tra le finalità di rilevante interesse pubblico e 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) erogazione di prestazioni sanitarie rese in ambito territoriale in materia di:
   - prevenzione a tutela della salute collettiva negli ambienti di vita e di lavoro;
   - salute mentale adulti, neuropsichiatria infantile ed adolescenza e dipendenze patologiche;
   - assistenza sanitaria di base, specialistica e riabilitativa, medicina legale e fiscale, farmaceutica;
   - attività veterinaria a garanzia dei livelli sanitari di sicurezza e di protezione della popolazione animale, igiene degli allevamenti e sicurezza ed integrità di prodotti alimentari di origine animale;

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

d) esercizio delle funzioni amministrative di competenza dell'Azienda:
   1. la gestione del personale dipendente, comprese le procedure di assunzione;
   2. la gestione dei soggetti che intrattengono rapporti giuridici con l'Azienda, diversi dal rapporto di lavoro dipendente e che operano a qualsiasi titolo all'interno dell'Azienda stessa, ivi compresi gli specializzandi, gli allievi e i docenti di corsi, i consulenti, i tirocinanti, i volontari;
   3. la gestione dei rapporti con i fornitori per l'approvvigionamento di beni e 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. la gestione del contenzioso instaurato nei confronti dell'Azienda, dei rapporti con i

legali e consulenti di parte;

6. i 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 Azienda; per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 5 – Condizioni per il Consenso

Ai sensi art.7 del Regolamento UE 2016/679, qualora il trattamento dei dati sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche 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 in qualsiasi momento. La revoca del consenso 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.

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.

Art. 7 – Trattamento di categorie particolari di dati personali

E' vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il precedente paragrafo non si applica qualora si verifichi uno dei seguenti casi:

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 del Regolamento UE 2016/679 (GDPR), 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. 8 – Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi a condanne penali e reati deve svolgersi secondo quanto previsto dell'art.10 del R.E. e dall'art.2 *octies* del Codice della Privacy n.196/2003. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

I dati particolari e giudiziari individuati nel presente regolamento sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie nel caso in cui la raccolta non avvenga presso l'interessato.

Le operazioni di interconnessione, raffronto, comunicazione e diffusione individuate nel presente regolamento sono ammesse soltanto se indispensabili allo svolgimento degli obblighi o compiti di volta in volta indicati, per il perseguimento delle finalità di interesse pubblico specificate e nel rispetto delle disposizioni rilevanti in materia di protezione dei dati personali, nonché degli altri limiti stabiliti dalla legge e dai regolamenti. I dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali sono inutilizzabili.

Art. 9 – Categorie di dati

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

- utenti, assistiti, pazienti e loro familiari e/o accompagnatori
- personale sanitario, amministrativo, tecnico e professionale della dirigenza e del comparto in rapporto di dipendenza, convenzione o collaborazione;
- soggetti che per motivi di studio, tirocinio, consulenza, stage o volontariato frequentano le

strutture dell'Azienda ed effettuano trattamento di dati personali;

- clienti e imprese che intrattengono rapporti con l'Azienda 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'Azienda 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;
- anche presso banche dati nazionali o regionali di libero accesso o ad accesso riservato.

Art. 10 – Emergenze e tutela della salute e dell'incolumità fisica

Le informazioni di cui agli articoli 13 e 14 del Regolamento UE 2016/679 possono essere rese senza ritardo, successivamente alla prestazione, nel caso di emergenza sanitaria o di igiene pubblica per la quale la competente autorità ha adottato un'ordinanza contingibile ed urgente ai sensi dell'articolo 117 del decreto legislativo 31/3/1998, n.112. Tali informazioni possono altresì essere rese senza ritardo, successivamente alla prestazione, in caso di: a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile rendere le informazioni, nei casi previsti, a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi dell'articolo 4 della legge 22 dicembre 2017, n. 219 o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato; b) rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato. Le informazioni di cui al comma 1 possono essere rese senza ritardo, successivamente alla prestazione, anche in caso di prestazione medica che può essere pregiudicata dal loro preventivo rilascio, in termini di tempestività o efficacia. Dopo il raggiungimento della maggiore età le informazioni sono fornite all'interessato nel caso in cui non siano state fornite in precedenza.

Art. 11 – Informazioni per la raccolta dei dati

L'Azienda, quale titolare del trattamento, adotta misure appropriate per fornire all'interessato tutte le informazioni e comunicazioni riguardanti il trattamento dei dati quali l'identità ed i dati di contatto del titolare del trattamento, i dati di contatto del responsabile della protezione dei dati, le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento, i legittimi interessi perseguiti dal titolare del trattamento o dai terzi, gli eventuali destinatari dei dati personali.

Nel momento in cui i dati personali sono ottenuti, il Titolare fornisce all'interessato ulteriori informazioni per garantire un trattamento corretto e trasparente quali:

a) l'identità ed i dati di contatto del titolare del trattamento;

b) i dati di contatto del responsabile della protezione dei dati;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

e) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;

f) il periodo di conservazione dei dati personali, oppure se non è possibile, i criteri utilizzati per determinare tale periodo;

g) l'esistenza del diritto dell'interessato di chiedere al titolare 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, oltre al diritto alla portabilità dei dati;

h) l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

i) il diritto di proporre reclamo ad un'autorità di controllo;

j) 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;

k) 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.

L'informativa all'interessato viene fornita per iscritto, anche per estratto, tramite materiale informativo reso disponibile in luoghi comuni dell'Azienda e presso l'apposita sezione del portale web http://www.ospedaliriunitipalermo.it/.

Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente dell'Azienda 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'Azienda 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

Qualora i dati non siano stati ottenuti presso l'interessato, l'Azienda fornisce all'interessato le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) le categorie di dati personali in questione;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali.

Oltre alle informazioni di cui al paragrafo 1, l'Azienda fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), Regolamento UE 2016/679 i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

c) 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 dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a) Regolamento UE 2016/679, oppure sull'articolo 9, paragrafo 2, lettera a), Regolamento UE 2016/679 l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;

e) il diritto di proporre reclamo a un'autorità di controllo;

f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, Regolamento UE 2016/679 e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

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

Art. 12 - Titolare del trattamento

L'Azienda, rappresentata ai fini previsti dal Regolamento UE 2016/679 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** di cui all'art.2- *quaterdecies* del Codice Privacy.

Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 Regolamento UE 2016/679: 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 Regolamento UE 2016/679. 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 Regolamento UE 2016/679, 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 Regolamento UE 2016/679, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art.14 Regolamento UE 2016/679, 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, 78, 79, 80, 82, 89-bis 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 Regolamento UE 2016/679, considerati: la natura, l'oggetto, il contesto e le finalità del medesimo trattamento. 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 da personale che opera sotto la sua autorità diretta e nell'ambito dell'assetto organizzativo aziendale, provvede a designare i Responsabili del trattamento o delegati a norma del citato art.2-*quaterdecies* del Codice della Privacy, come previsto dall'art.26 dell'Atto Aziendale adottato dall'Azienda con deliberazione n.631 del 30/9/2019 e successiva n.142 del 30/1/2020. Ai sensi del medesimo art.2-*quaterdecies* del Codice Privacy, è consentita la nomina di sub-delegati del trattamento da parte di ciascun Responsabile delegato per specifiche attività di trattamento, nel rispetto degli stessi obblighi che legano il Titolare ed il Responsabile delegato; le operazioni di trattamento possono essere effettuate solo dal personale autorizzato che opera sotto la diretta autorità del Responsabile delegato, attenendosi alle indicazioni loro impartite per iscritto che

individuano specificatamente l'ambito del trattamento consentito. Il Responsabile delegato risponde, anche dinanzi al Titolare, dell'operato dei sub-delegati 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-delegato. Il Responsabile delegato 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, l'accesso ai dati trasmessi o comunque trattati. Il Responsabile 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 o abbia un adeguato obbligo legale di riservatezza.

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 Regolamento UE 2016/679. 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 Regolamento UE 2016/679, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
Il Titolare ha designato il Responsabile della Protezione dei dati (D.P.O.) di cui agli artt.37-39 Regolamento UE 2016/679, il quale redige, custodisce ed aggiorna il Registro delle attività di trattamento, a norma dell'art.30 del Regolamento UE 2016/679; provvede alla notifica all'autorità di controllo in caso di violazione dei dati personali art.33 Regolamento UE 2016/679.

Art. 13 – Responsabili esterni del trattamento

Qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre unicamente ai Responsabili del trattamento secondo quanto previsto dall'art.28, Regolamento UE 2016/679, che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate. Questi trattamenti sono disciplinati, a norma dello stesso art.28, par. 3, da un contratto o altro atto giuridico che vincoli il responsabile del trattamento al Titolare. Il contratto o accordo quadro può essere firmato dal Titolare o da un suo delegato. Gli originali sono custoditi dal Titolare o dal delegato e copia viene inviata all'Ufficio Privacy dell'Azienda, già costituto con deliberazione n.657 del 3/10/2019, che aggiorna l'elenco dei Responsabili esterni anche per permettere eventuali audit. 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, 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 o abbia un adeguato obbligo legale di riservatezza.

Il Responsabile si impegna inoltre ai sensi dell'art.28, comma 3, lett. F), Regolamento UE 2016/679, 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 Regolamento UE 2016/679 o di comunicazione della stessa agli interessati a norma dell'art.34 Regolamento UE 2016/679. La comunicazione dovrà avvenire a mezzo PEC all'indirizzo protocollo@pec.ospedaliriunitipalermo.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'Azienda.

Art. 14 - Registro delle attività di trattamento

Il Titolare del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità, costantemente aggiornato, e contiene almeno le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento 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.

Ogni responsabile del trattamento tiene un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare 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. 15 - 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, 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.

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'Azienda 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'Azienda, 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'Azienda Ospedaliera "Ospedali Riuniti Villa Sofia Cervello di Palermo: http://www.ospedaliriunitipalermo.it/.

Art. 16 - Violazione dei dati personali – notifica e comunicazione

Una violazione di dati personali è: *ogni infrazione alla sicurezza degli stessi che comporti - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal Titolare del trattamento.* La violazione di dati è un tipo particolare di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del Regolamento UE 2016/679.

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

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

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

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

In particolari circostanze le violazioni potrebbero essere combinate tra loro.

Il Responsabile e/o l'incaricato del trattamento sono tenuti ad informare senza ingiustificato ritardo l'Azienda 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'Azienda avvia le necessarie procedure e, avvalendosi della collaborazione del Responsabile del trattamento e del DPO, accerta l'effettivo stato dell'arte.

L'Azienda 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.

Valutata la necessità di effettuare o meno la notifica della violazione dei dati, l'Azienda, procede senza ritardo secondo le modalità stabilite dagli artt.33 e 34 del Regolamento UE 2016/679. Indipendentemente dalla necessità della comunicazione all'Autorità di controllo ed all'interessato, il Titolare ha predisposto un Registro di Data Breach, tenuto anche dal Responsabile delle Protezione dei dati, contenente:

- ☐ il numero della violazione;
- ☐ la data della violazione;
- ☐ la natura della violazione;
- ☐ la categoria degli interessati;

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

Art. 17 - Valutazione d'impatto sulla protezione dei dati e 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, il Titolare, prima di procedere al trattamento dei dati personali, effettua una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali consultandosi con il Responsabile della Protezione dei Dati. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi analoghi. La DPIA sarà condotta in tutti quei casi previsti dal Provvedimento del Garante pubblicato in Gazzetta ufficiale n°269 del 19/11/2018.

La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dall' Azienda;

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;

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

Se necessario l'Azienda 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'Azienda prima di procedere al trattamento consulta il Garante della Privacy, avvalendosi del supporto del DPO, ai sensi di quanto disposto dall'art.36 Regolamento (UE) 2016/679.

Art. 18 – Responsabile della protezione dei dati

Il Responsabile della Protezione dei Dati, o Data Protection Officer (DPO), è designato dall'Azienda 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'Azienda ha provveduto, in ottemperanza a quanto disposto dall'art.37 e ss. Regolamento UE 2016/679 al conferimento dell'incarico di Responsabile della protezione dei dati.

Il DPO è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 e dalle altre disposizioni vigenti relative alla protezione dei dati. In tal senso il DPO può indicare al Titolare e agli Autorizzati 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 Regolamento UE 2016/679 e delle altre normative relative alla protezione dei dati;

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 DPO 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 Regolamento UE 2016/679;

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 Regolamento UE 2016/679, 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) può, insieme al Titolare, tenere i registri delle attività di trattamento;

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.

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

Il Titolare ed il Responsabile del trattamento assicurano che il Responsabile della Protezione dei Dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

A tal fine:

- il DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il DPO 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 DPO 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 DPO, è necessario motivare specificamente tale decisione;
- il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

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

Il DPO coordina l'Ufficio Protezione dei dati, costituto con deliberazione n.657 del 3/10/2019, ed il Gruppo di lavoro per la protezione dei dati, costituto con deliberazione n.656 del 3/10/2019, ed opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il DPO 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 DPO riferisce direttamente al Titolare o suo delegato o al Responsabile del trattamento. Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il Regolamento UE 2016/679 e con le indicazioni fornite dallo stesso DPO, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.
Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

Art. 19 - L'interessato

L'interessato (*data subject*) al trattamento è la **persona fisica** cui si riferiscono i dati personali. La normativa attribuisce specifici diritti all'interessato, il quale, per l'esercizio di tali diritti, può rivolgersi direttamente al Titolare del trattamento attraverso l'apposita modulistica che potrà essere richiesta presso l'URP oppure scaricata dal sito Internet dell'Azienda all'indirizzo http://www.ospedaliriunitipalermo.it/. Può esercitare i suoi diritti anche in un momento successivo a quello in cui ha prestato il consenso, potendo così revocare un consenso già prestato.

I diritti esercitabili dall'interessato sono i seguenti:

- di ottenere informazioni su quali dati sono trattati dal titolare sia se ottenuti presso l'interessato che se non ottenuti presso l'interessato (diritto di informazione);
- di chiedere ed ottenere in forma intellegibile i dati in possesso del titolare (diritto di accesso);
- di revocare il consenso in qualsiasi momento;
- di opporsi al trattamento in tutto o in parte;
- di ottenere la cancellazione dei dati in possesso del titolare (diritto all'oblio);
- di ottenere l'aggiornamento o la rettifica dei dati conferiti;
- di chiedere ed ottenere la trasformazione in forma anonima dei dati;
- di chiedere ed ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento;
- portabilità dei dati.

Art. 20 - 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. 21 - 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'Azienda fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, l'Azienda 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. 22 - 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. 23 - Diritto alla cancellazione (diritto all'oblio)

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. 24 – Diritto di limitazione del trattamento

Il diritto di limitazione (art. 18 del regolamento) consente all'interessato di ottenere il blocco del trattamento nelle seguenti ipotesi:

- l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'interessato si è opposto al trattamento ai sensi dell'art. 21, paragrafo 1 Regolamento (UE) 2016/679, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato. In caso di esercizio di tale diritto ogni trattamento, tranne la conservazione è vietato.

Art. 25 – Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Art. 26 - 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. 27 - Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano e l'Azienda 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. 28 - Personale autorizzato al trattamento dei dati personali

I **soggetti autorizzati al trattamento dei dati personali** (SATD), ex art. 2-*quaterdecies* del Codice della Privacy, 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 alla designazione di altri Autorizzati (Autorizzati/Incaricati). In questo caso, la delega alla nomina dovrà essere contenuta nell'atto di designazione e riportata nell'atto di nomina dell'Autorizzato/Incaricato.
Possono essere altresì autorizzati i soggetti che a qualsiasi titolo (ad esempio: tirocinanti, studenti, volontari, libero professionisti, consulenti, ecc.), prestino la loro opera, anche in via temporanea, all'interno delle strutture dell'Azienda in attività che comportano il trattamento di dati personali per conto dell'Azienda.
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 Regolamento UE 2016/679;
- forniscono al DPO le informazioni utili all'aggiornamento del registro dei trattamenti;
- informano il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati.

Art. 29 - Amministratore di sistema

L'Azienda 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'Azienda;
- 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'Azienda 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. 30 – Sicurezza e conservazione dei dati

L'Azienda adotta misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato). Tra tali misure vi sono (art. 32 Codice UE):

a) pseudonimizzazione e la cifratura dei dati;

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 ed organizzative al fine di garantire la sicurezza del trattamento.

L'Azienda assicura inoltre, ai fini di una corretta conservazione 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'Azienda.
- 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'Azienda.

Art. 31 - Misure organizzative per la tutela della riservatezza

Presso tutti i Presidi e le Strutture dell'Azienda 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. 32 - Consenso al trattamento dei dati personali – modalità di rilascio e conservazione

Il Titolare assicura attraverso idonee modalità l'archiviazione dei consensi espressi dagli interessati, di cui all'art. 5 del presente Regolamento, 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'Azienda organizza modalità atte a facilitare l'espressione del consenso da parte dell'interessato, secondo le modalità e le forme previste dalla normative vigente.

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

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

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

Art. 33 - Attività di verifica e controllo

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

Art. 34 – Formazione

L'Azienda, nel rispetto dell'art. 32 del GDPR "Sicurezza del trattamento" paragrafo 4 che prevede che *"il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità*

e abbia accesso a dati personali non tratti tali dati se **non è istruito in tal senso dal Titolare del trattamento"** propone ai propri collaboratori delle sedute formative periodiche per promuovere la cultura della protezione dei dati e per l'aggiornamento informatico giuridico conseguente alle diverse modalità di trattamento. Le attività di formazione possono prevedere anche dei focus mirati su argomenti specifici indirizzati anche a singole unità di personale.

Art. 35 - Attività di sensibilizzazione

L'Azienda promuove al suo interno anche attività di sensibilizzazione che possano consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.
In tale ottica una delle iniziative di sensibilizzazione sono costituite da attività informative rivolte non solo al personale ma anche coloro che hanno rapporti, a vario titolo con l'Azienda.
Oltre a specifiche attività formative finalizzate al continuo aggiornamento del personale autorizzato al trattamento dei dati personali, come previsto dall'art. 34 del presente Regolamento, l'Azienda, al fine di garantire la conoscenza capillare delle disposizioni contenute nel Regolamento UE e nel presente documento, ha previsto un'area, all'interno del proprio portale web, accessibile dalla Home Page del sito, dedicata al tema della protezione dei dati personali contenente, oltre al presente documento, la normativa di riferimento, la modulistica da usare nello svolgimento delle attività istituzionali e ogni altra documentazione di supporto.
Inoltre, ad ogni nuova Unità di Personale viene consegnata una specifica comunicazione con i riferimenti per l'acquisizione e la consultazione del presente Regolamento. Il dipendente, acquisita tale comunicazione, si impegna a scaricarne copia, prendere visione ed attenersi alle prescrizioni Azienda in materia di protezione dei dati personali.

Art. 36 - Il trattamento dei dati del personale

L'Azienda 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'Azienda 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'Azienda gestisce il 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 edalle Linee Guida del Garante per la protezione dei dati personali.

Art. 37 - Reclutamento del personale

Nelle procedure di reclutamento di nuove unità di personale l'Azienda provvede a corredare la documentazione necessaria con un'informazione trasparente sulle modalità di trattamento dei dati dei candidati. Viene richiesto uno specifico consenso al trattamento e viene chiesto di fornire due curricula: il primo completo di tutti dati identificativi, eventualmente anche di natura particolare (appartenenza a categorie protette) o giudiziari, del soggetto partecipante al bando di selezione; un secondo contenente solo il nome e cognome dell'interessato ed epurato di qualunque altro dato (residenza, numero di telefono, codice fiscale ecc...). Quest'ultimo sarà quello che verrà sottoposto a pubblicazione se previsto dalla legge.

Art. 38 – Pubblicazione graduatorie

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

Art. 39 – Pubblicazione albo on line

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 privati, indirizzo di residenza, carta d'identità, patologie, dati del casellario giudiziale, conti correnti bancari etc..), 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 nella documentazione allegata all'originale integrale del documento a disposizione degli uffici competenti e del personale appositamente autorizzato.

Art. 40 – Il diritto di accesso e il diritto alla riservatezza

L'Azienda, 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. 41 – Pubblicazione nell'Amministrazione trasparente

Salvo diversa disposizione di legge, i documenti da pubblicare sul sito istituzionale per finalità di trasparenza e/o pubblicità non devono consentire l'identificabilità dei soggetti cui i dati si riferiscono quando contengono dati non necessari alla divulgazione, dati di natura particolare, dati giudiziari o di minori. Per quanto sopra, ciascun Ufficio competente alla redazione e conservazione del documento verifica caso per caso, con l'ausilio ove necessario del Responsabile della Protezione dei Dati, e seguendo le istruzioni impartite dalla

Direzione Generale, la presenza di eventuali dati da oscurare o rendere anonimi o da pseudonimizzare (quali a titolo esemplificativo ma non esaustivo, numeri telefonici private, indirizzo di residenza, carta d'identità, patologie, dati del casellario giudiziale), procedendo in tal caso a curare la omissione dei medesimi dati dal contenuto del documento, prima di trasmettere il medesimo per la relativa pubblicazione al soggetto addetto a tale attività. Per assicurare comunque la completezza delle deliberazioni, i dati personali da escludere dalla pubblicazione sono contenuti nell'originale integrale del documento a disposizione degli uffici competenti e del personale appositamente autorizzato

Art. 42 - Informazioni del medico o del pediatra

Il medico o il pediatra informa l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati negli articoli 13 e 14 del Regolamento UE 2016/679.

Le informazioni possono essere fornite per il complessivo trattamento dei dati personali necessario per attività di diagnosi, assistenza e terapia sanitaria, svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.

Le informazioni possono riguardare, altresì, dati personali eventualmente raccolti presso terzi e sono fornite preferibilmente per iscritto

Le informazioni, se non è diversamente specificato dal medico o dal pediatra, riguardano anche il trattamento di dati correlato a quello effettuato dal medico o dal pediatra, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che:

a) sostituisce temporaneamente il medico o il pediatra;

b) fornisce una prestazione specialistica su richiesta del medico e del pediatra;

c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata;

d) fornisce farmaci prescritti;

e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile.

Le informazioni rese ai sensi del presente articolo evidenziano analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati:

a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;

b) nell'ambito della teleassistenza o telemedicina;

c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica;

c-bis) ai fini dell'implementazione del fascicolo sanitario elettronico di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;

c-ter) ai fini dei sistemi di sorveglianza e dei registri di cui all'articolo 12 del decreto legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.

Art. 43 – Informazioni da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio – sanitarie

Le strutture pubbliche e private, che erogano prestazioni sanitarie e sociosanitarie possono avvalersi delle modalità particolari di cui all'articolo precedente in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti ed unità della stessa struttura o di sue articolazioni ospedaliere o territoriali specificamente identificate.

Nei casi di cui al comma 1 la struttura o le sue articolazioni annotano l'avvenuta informazione con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità che, anche in tempi diversi, trattano dati relativi al medesimo interessato.

Art. 44 – Prescrizione di medicinali

Per le prescrizioni di medicinali, laddove non è necessario inserire il nominativo dell'interessato, si adottano cautele particolari in relazione a quanto disposto dal Garante nelle misure di garanzia di cui all'articolo 2-septies del Dlgs 196/2003, anche ai fini del controllo della correttezza della prescrizione ovvero per finalità amministrative o per fini di ricerca scientifica nel settore della sanità pubblica.

Art. 45 – Cartelle cliniche

La Cartella Clinica è uno strumento di lavoro che permette attraverso il diario giornaliero, la sistematica raccolta cronologica, logica e obiettiva delle informazioni sul paziente continuamente aggiornate, necessarie

a formulare diagnosi più efficienti ed efficaci e alla progettazione del piano assistenziale definito per obiettivi da raggiungere.

Per la redazione e la conservazione della cartella clinica in conformità alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

a) di esercitare o difendere un diritto in sede giudiziaria ai sensi dell'articolo 9, paragrafo 2, lettera f), del Regolamento UE 2016/679, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale;

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale.

Art. 46 – Certificato di assistenza al parto

Ai fini della dichiarazione di nascita il certificato di assistenza al parto è sempre sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita. Per la rilevazione dei dati statistici relativi agli eventi di nascita, compresi quelli relativi ai nati affetti da malformazioni e ai nati morti, nonché per i flussi di dati anche da parte di direttori sanitari, si osservano, oltre alle disposizioni di cui al decreto del Ministro della sanità 16 luglio 2001, n. 349, le modalità tecniche determinate dall'Istituto nazionale di statistica, sentiti i Ministri della salute, dell'interno e il Garante.

Il certificato di assistenza al parto o la cartella clinica, ove comprensivi dei dati personali che rendono identificabile la madre che abbia dichiarato di non voler essere nominata avvalendosi della facoltà di cui all'articolo 30, comma 1, del decreto del Presidente della Repubblica 3 novembre 2000, n. 396, possono essere rilasciati in copia integrale a chi vi abbia interesse, in conformità alla legge, decorsi cento anni dalla formazione del documento.

Durante il periodo di cui al comma precedente, la richiesta di accesso al certificato o alla cartella può essere accolta relativamente ai dati relativi alla madre che abbia dichiarato di non voler essere nominata, osservando le opportune cautele per evitare che quest'ultima sia identificabile.

Art. 47 – Fascicolo sanitario elettronico

Il fascicolo sanitario elettronico (FSE) è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito.

Il FSE è istituito, a fini di:

a) prevenzione, diagnosi, cura e riabilitazione;

b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico;

c) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria.

Il FSE è alimentato in maniera continuativa, dai soggetti che prendono in cura l'assistito nonché, su richiesta del cittadino, con i dati medici in possesso dello stesso.

Il FSE può essere alimentato esclusivamente sulla base del consenso libero e informato da parte dell'assistito, il quale può decidere se e quali dati relativi alla propria salute non devono essere inseriti nel fascicolo medesimo.

La consultazione dei dati e documenti presenti nel FSE, per le finalità di cui alla lettera a) del comma precedente, può essere realizzata soltanto con il consenso dell'assistito e sempre nel rispetto del segreto professionale, salvo i casi di emergenza sanitaria secondo modalità individuate a riguardo. Il mancato consenso non pregiudica il diritto all'erogazione della prestazione sanitaria.

La consultazione dei dati e documenti presenti nel FSE, può essere realizzata soltanto in forma protetta e riservata secondo modalità determinate. Le interfacce, i sistemi e le applicazioni software adottati devono assicurare piena interoperabilità' tra le soluzioni secondo modalità determinate. Con decreto del Ministro della salute e del Ministro delegato per l'innovazione tecnologica, di concerto con il Ministro per la pubblica amministrazione e la semplificazione e il Ministro dell'economia e delle finanze, sentita la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, acquisito il parere del Garante per la protezione dei dati personali, ai sensi dell'articolo 154, comma 4, del decreto legislativo 30 giugno 2003, n. 196, sono stabiliti: i contenuti del FSE e i limiti di responsabilità e i compiti dei soggetti che concorrono alla sua implementazione, i sistemi di codifica dei dati, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito, le modalità e i livelli diversificati di accesso al FSE da parte dei soggetti, la definizione e le relative modalità di attribuzione di un codice identificativo univoco dell'assistito che non consenta l'identificazione diretta dell'interessato, i criteri per l'interoperabilità del FSE a livello regionale, nazionale ed europeo, nel rispetto delle regole tecniche del sistema pubblico di connettività.

I sistemi di sorveglianza e i registri di mortalità, di tumori e di altre patologie, di trattamenti costituiti da trapianti di cellule e tessuti e trattamenti a base di medicinali per terapie avanzate o prodotti di ingegneria

tessutale e di impianti protesici sono istituiti ai fini di prevenzione, diagnosi, cura e riabilitazione, programmazione sanitaria, verifica della qualità delle cure, valutazione dell'assistenza sanitaria e di ricerca scientifica in ambito medico, biomedico ed epidemiologico allo scopo di garantire un sistema attivo di raccolta sistematica di dati anagrafici, sanitari ed epidemiologici per registrare e caratterizzare tutti i casi di rischio per la salute, di una particolare malattia o di una condizione di salute rilevante in una popolazione definita

Art. 48 – Modalità di trattamento pazienti

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

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). **E' vietato ai pazienti fare fotografie o riprese video nei reparti**. Il personale è tenuto a vigilare sul rispetto di questo divieto.

Durante lo svolgimento di colloqui con il personale sanitario ad es. in occasione di prescrizioni o di certificazioni mediche etc.., (che devono avvenire in locali riservati) vanno 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.

La notizia o la conferma di una prestazione, della presenza o del passaggio di una persona al pronto soccorso, possono essere fornite correttamente ai soli terzi legittimati, quali possono essere familiari, parenti o conviventi, nominativamente indicati dall'Interessato, nell'acquisizione del consenso al trattamento dei dati, se non impossibilitato e valutate le diverse circostanze del caso. Il personale Autorizzato deve accertare l'identità dei terzi legittimati a ricevere la predetta notizia o conferma, avvalendosi anche di elementi desunti dall'Interessato. Le informazioni che possono essere fornite riguardano solo la circostanza che è in atto o si è svolta una prestazione di pronto soccorso e non anche informazioni più dettagliate sullo stato di salute

dell'Interessato. L'Interessato - se cosciente e capace - deve essere preventivamente informato (ad. es. in fase di accettazione) e posto in condizione di fornire indicazioni circa i soggetti che possono essere informati della prestazione di pronto soccorso. Occorre altresì rispettare eventuali sue indicazioni specifiche o contrarie.

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

Art. 49— Utilizzo hardware e software

Il Personal Computer o il pc portatile affidati al dipendente sono uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può determinare un livello di sicurezza non adeguato oltre a disservizi e costi di manutenzione.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato, il tutto coma da apposita disposizione interna n.13589/1 del 28/10/2019.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo autorizzazione esplicita del Responsabile dei sistemi informatici aziendali, in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Responsabile dei sistemi informatici dell'Azienda. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del Responsabile dei sistemi informatici aziendali.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del Responsabile dei sistemi informatici aziendali.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile dei sistemi informatici aziendali nel caso in cui vengano rilevati virus.

Art. 50—Utilizzo della rete

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

Il Responsabile dei sistemi informatici aziendali può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

Art 51 — Rilascio credenziali di autenticazione

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal Responsabile dei sistemi informatici aziendali.

E' necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di

dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al Responsabile dei sistemi informatici aziendali.

La password deve essere immediatamente sostituita, dandone comunicazione al Responsabile dei sistemi informatici aziendali, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a dare immediata notizia alla Direzione o al Responsabile dei sistemi informatici aziendali.

Art. 52 — Uso della posta elettronica della Rete Internet e dei relativi servizi

La casella di posta assegnata dall'Azienda all'utente ed il PC abilitato alla navigazione in Internet sono strumenti di lavoro, ogni utilizzo non inerente all'attività lavorativa può determinare un livello di sicurezza non adeguato oltre a disservizi e costi di manutenzione. Le persone assegnatarie delle caselle di posta elettronica e della rete internet sono responsabili del corretto utilizzo delle stesse. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

Disposizioni finali

Art. 53 - Responsabilità in caso di violazione delle disposizioni in materia di privacy

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

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. 54 – Abrogazione regolamento precedente

Il presente regolamento entra in vigore ad intervenuta esecutività della relativa delibera di approvazione, in sostituzione di ogni precedente regolamentazione interna nella medesima materia e viene pubblicato nel sito

istituzionale: http://www.ospedaliriunitipalermo.it/ nella sezione "Amministrazione Trasparente" e nella sezione "Privacy e Protezione dei dati".

La sostituzione dei nominativi individuati nelle deliberazioni di nomina di funzioni varie indicate nel presente Regolamento non comporta l'esigenza di apportare formali modifiche allo stesso Regolamento.

Art. 55 - Rinvio a disposizioni di legge

Per quanto non espressamente previsto nel presente regolamento, si fa rinvio al Regolamento Europeo 2016/679 del 27/4/2016 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.

VERBALE N. 2 DEL 17.02.2020

In data odierna alle ore 09.30 si è riunito il Gruppo di lavoro a supporto del Data Protection Officier, costituito ai sensi della deliberazione n. 656 del 03.10.2019 a seguito di mail di convocazione del 12.02.2020 per discutere il seguente O.d.g.:

1. Esame bozza "Regolamento per la protezione dati personale";
2. Esame bozza integrazione disposizioni interne di cui alla nota 13211-COMM del 18.06.2018

Sono presenti:
Il Sig. Michele Ruggiano, Coordinatore del Gruppo di lavoro DPO, nominato a seguito di deliberazione n. 991 del 24.12.2019;
La Dr.ssa Rosalia Sensale, Direzione Medica P.O. Cervello;
La Dr.ssa Anna Lavima, Direzione Medica P.O. Villa Sofia;
L'Avv.to Sergio Buccellato, Servizio Legale;
Svolge le funzioni di segretario verbalizzante la Sig.ra Cuntrera Sabrina.

Su invito del Coordinatore, per competenza istruttoria riguardante il documento in esame del punto 2. dell'o.d.g., è stata invitata l'RPCT aziendale, Dr.ssa Maria Ilaria Dilena che per altri impegni istituzionali non può partecipare.

Il Coordinatore espone sinteticamente le attività sinora poste in essere dalla data di nomina, evidenziando, in particolare, di avere istituito il protocollo per la posta in entrata e in uscita dell'Ufficio Protezioni Dati, il Registro delle Violazioni e di avere avviato la predisposizione del Registro dei Trattamenti. Sottolinea l'importanza della Formazione per tutti i dipendenti, vista la delicatezza dell'argomento, al fine di promuovere la cultura della protezione dei dati in Azienda, sulla scorta delle previsioni della norme in esame, dell'atto Aziendale adottato, nonché della bozza di Regolamento in esame.

Per il Punto 1 dell'o.d.g.: Si specifica che la bozza del Regolamento di che trattasi era stato già inviato al Gruppo di lavoro per una attenta disamina già nel mese di dicembre 2019. Il Coordinatore ha apportato

SITO WEB: www.ospedaliriunitipalermo.it
SEDE LEGALE: Viale Strasburgo, 233 90146 – Palermo
D.P.O. Viale Strasburgo, 233 90146 – Palermo Tel.: +39 091 / 780(8792) – (8302)

una serie di integrazioni e modifiche allo stesso che rimette all'esame del Gruppo, al fine di avviare i processi organizzativi previsti dalla vigente normativa in materia di privacy (GDPR). Alcune integrazioni riguardano fondamentalmente il richiamo all'organizzazione aziendale dei vari organismi e uffici interni costituiti (Atto aziendale, delibere di costituzione del Gruppo di lavoro DPO e dell'Ufficio Trattamento Dati, il conformarsi alle norme e all'organizzazione aziendale).

Per quanto riguarda la modulistica, richiamata nel Regolamento, il Gruppo di lavoro ritiene opportuno di non richiamarla come parte integrante dello stesso Regolamento, bensì rinviarne il reperimento sul sito web aziendale.

Dopo attenta lettura di tutte le modifiche ed integrazioni effettuate nella Bozza di Regolamento, i presenti condividono i nuovi contenuti e rinviano la stessa bozza condivisa alla Direzione Aziendale per la successiva approvazione, (Allegato 1 al presente verbale), tramite schema di deliberazione che predisporrà e proporrà il DPO.

Per il Punto 2 dell'o.d.g.: Il Coordinatore, è stato coinvolto, unitamente all'RPCT, dalla Direzione Strategica, a predisporre un provvedimento finalizzato a chiarire le modalità di corredo documentale delle deliberazioni adottate, per renderle effettivamente compatibili al contesto normativo vigente in materia di privacy / trasparenza, tenuto conto degli obblighi di pubblicazione delle stesse deliberazioni.
Il Coordinatore legge e rimette all'esame dei presenti la bozza di documento predisposta, della quale la direzione Aziendale ha già preso visione, che viene condivisa dal Gruppo per quanto attiene la normativa sulla privacy (Allegato n. 2 al presente verbale).
La riunione si chiude alle ore 12.30, il presente verbale verrà trasmesso alla Direzione Strategica per la dovuta conoscenza.
Il presente verbale, letto e confermato, viene sottoscritto come segue.
Il Coordinatore, Michele Ruggiano
Sig.ra Sabrina Cuntrera Segretario Verbalizzante

Palermo, 17.02. 2020

SITO WEB:
www.ospedaliriunitipalermo.it
SEDE LEGALE:
Viale Strasburgo, 233
90146 – Palermo
D.P.O.
Viale Strasburgo, 233
90146 – Palermo
Tel.: +39 091 / 780(8792) – (8302)

VERBALE N. 3 DEL 24.02.2020

In data odierna alle ore 09.30 si è riunito il Gruppo di lavoro a supporto del Data Protection Officier, costituito ai sensi della deliberazione n. 656 del 03.10.2019 a seguito di mail di convocazione del 20.02.2020 per discutere il seguente O.d.g.:

1. Riesame del "Regolamento per la protezione dati personale, a seguito di sostanziali modifiche apportate agli artt. 12 e 13 della bozza di Regolamento esitata nella riunione del 17.02.2020;
2. Varie ed eventuali.

Sono presenti:

Il Sig. P.i.Michele Ruggiano, Coordinatore del Gruppo di lavoro DPO, nominato a seguito di deliberazione n. 991 del 24.12.2019;

La Dr.ssa Anna Lavima, Direzione Medica P.O. Villa Sofia;

La Dr.ssa Daniela Gizzi, Collaboratore Amministrativo;

L'Avv.to Sergio Buccellato, Servizio Legale;

Svolge le funzioni di segretario verbalizzante la Sig.ra Cuntrera Sabrina.

La Dr.ssa Rosalia Sensale, Direzione Medica P.O. Cervello, assente per motivi di salute;

Il Dr. Antonio Todaro, Anticorruzione e Trasparenza, assente per congedo ordinario.

Il Coordinatore espone sinteticamente che a seguito di riunione in Assessorato del Gruppo di coordinamento regionale dei DPO ha ritenuto necessario apportare delle sostanziali modifiche agli artt. 12 e 13 della bozza di Regolamento in riesame, al fine di inquadrare correttamente le distinte fattispecie di "personale autorizzato ex art 2-*quaterdecies* del Codice privacy " e di Responsabile esterno del trattamento di cui all'art. 28 del GDPR.

Si procede pertanto alla lettura degli artt. modificati che il Gruppo di Lavoro, dopo ampia discussione, esita favorevolmente

La riunione si chiude alle ore 12.00, il presente verbale verrà trasmesso alla Direzione Strategica per la dovuta conoscenza.

www.ospedaliriunitipalermo.it
Viale Strasburgo, 233
90146 – Palermo
Viale Strasburgo, 233
90146 – Palermo
Tel.: +39 091 / 780(8792) – (8302)

Il presente verbale, letto e confermato, viene sottoscritto come segue.

Il Coordinatore, P.i. Michele Ruggiano

Sig.ra Sabrina Cuntrera Segretario Verbalizzante

Palermo, 24.02. 2020

www.ospedaliriunitipalermo.it
Viale Strasburgo, 233
90146 – Palermo
Viale Strasburgo, 233
90146 – Palermo
Tel.: +39 091 / 780(8792) – (8302)

AZIENDA OSPEDALIERA
OSPEDALI RIUNITI VILLA SOFIA - CERVELLO
PALERMO

DELIBERA DEL DIRETTORE GENERALE

PUBBLICAZIONE

Il sottoscritto dichiara che la presente deliberazione – ai sensi e per gli effetti dell'art. 53, comma 2, della L.R. n. 30/93 e dell'art. 32 della Legge n. 69/09 e s.m.i.– in copia conforme all'originale è stata pubblicata in formato digitale all'Albo on-line dell'Azienda Ospedaliera "*Ospedali Riuniti Villa Sofia – Cervello*", istituito sul sito www.ospedaliriunitipalermo.it, a decorrere dal giorno 01 MAR 2020 e che nei 15 giorni successivi:

☐ non sono pervenute opposizioni
☐ sono pervenute opposizioni da _____

L'ADDETTO
ALLA PUBBLICAZIONE

_____

IL FUNZIONARIO
INCARICATO

_____

Notificata al Collegio Sindacale il _____ prot. n. _____

DELIBERA NON SOGGETTA AL CONTROLLO

☐ Delibera non soggetta al controllo, ai sensi dell'art. 4, comma 8, della L. n. 412/1991 e divenuta:

ESECUTIVA
decorso il termine (10 giorni dalla data di pubblicazione) ai sensi dell'art. 53, comma 6, L.R. n. 30/93

☐ Delibera non soggetta al controllo, ai sensi dell'art. 4, comma 8, della L. n. 412/1991 e divenuta:

IMEDIATAMENTE ESECUTIVA
ai sensi dell'art. 53, comma 7, L.R. n. 30/93

IL FUNZIONARIO
INCARICATO

_____

ESTREMI RISCONTRO TUTORIO

☐ Delibera trasmessa, ai sensi della L.R. 5/09, all'Assessorato Regionale Salute n. in data

_____

prot. n. _____

SI ATTESTA
che l'Assessorato Regionale Salute, esaminata la presente Deliberazione:

☐ ha pronunciato l'approvazione con atto prot. n. _____ del _____ come da allegato.

☐ ha pronunciato l'annullamento con atto prot. n. _____ del _____ come da allegato.

☐ Delibera divenuta esecutiva per decorrenza del termine previsto dall'art. 16 della L.R. n. 5/09 dal

_____

IL FUNZIONARIO
INCARICATO

_____

Azienda Ospedaliera Ospedali Riuniti Villa Sofia - Cervello
REGIONE SICILIA