Azienda Ospedaliero Universitaria "Policlinico-Vittorio Emanuele"
Catania

Regolamento

Protezione dei dati personali

Agosto 2019

(Adottato con deliberazione n. 1509 del 10/09/2019)

Regolamento per la protezione dei dati personali

Regolamento (UE) 2016/679 del 27 aprile 2016

General Data Protection Regulation (GDPR)

D. Lgs. 30 giugno 2003 n. 196

Codice in materia di protezione dei dati personali

Agosto 2019

Indice

Premessa

L'Azienda Ospedaliero-Universitaria Policlinico – Vittorio Emanuele (d'ora in poi "l'Azienda") con il presente documento recepisce quanto disposto con il Regolamento (UE) 2016/679, Regolamento Generale sulla Protezione dei dati (d'ora in poi "GDPR"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, fornendo indicazioni per la creazione all'interno dell'Azienda di un sistema di gestione dei dati personali secondo il principio di accountability.

Con il Decreto Legislativo n. 101 del 10 agosto 2018, il Legislatore ha modificato la normativa nazionale rappresentata dal Decreto Legislativo n. 196/2003 (Codice in materia di protezione dei dati) adeguando le parti incompatibili o contrastanti con il GDPR.

Più in particolare, l'art. 2 quaterdecies del D. Lgs. 196/2003, introdotto dal D.Lgs. 101/2018, conferisce ai titolari e responsabili del trattamento la possibilità di prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Inoltre, la medesima norma prevede che il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

Scopo del presente documento è pertanto quello di definire il modello organizzativo e gestionale per il trattamento dei dati che l'Azienda Ospedaliero-Universitaria "Policlinico – Vittorio Emanuele" intende adottare alla luce delle modifiche normative sopra richiamate.

Principale normativa di riferimento

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati, GDPR);
- Decreto Legislativo 30/06/2003 n. 196, modificato con D.Lgs. n. 101 del 10/08/2018, "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.;
- Deliberazione del Garante per la protezione dei dati personali del 14/06/2007 "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico";
- Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, e s.m.i. "Misure e accorgimenti prescritti ai titolari del trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- Decreto del Presidente della Repubblica 16 aprile 2013 n. 62 "Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165";
- Decreto del Presidente del Consiglio dei Ministri 8 agosto 2013 "Modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali";
- Provvedimento del Garante per la protezione dei dati personali n. 393 del 2 luglio 2015 "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche";
- Provvedimento del Garante per la protezione dei dati personali n. 515 del 19 dicembre 2018 "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica" e n. 512 del 19 dicembre 2018 "Regole deontologiche relative al trattamento di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria".

- Provvedimento del Garante per la protezione dei dati personali n. 55 del 7 marzo 2019 "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario".
- Provvedimento del Garante per la protezione dei dati personali n. 146 del 5 giugno 2019 "Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1, del D. Lgs. 10 agosto 2018 n. 101".

Definizioni

Si richiamano di seguito alcune delle definizioni contenute nell'art. 4 del GDPR:

- **«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;
- **«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;
- **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- **«profilazione»**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **«pseudonimizzazione»**: il trattamento 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;
- **«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;
- **«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;
- **«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;
- **«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;
- **«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;
- **«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;
- **«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;

- **«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;
- **«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;
- **«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;

Parte prima – Il trattamento dei dati

Art. 1 - Oggetto ed ambiti di applicazione

Il presente documento disciplina le modalità con cui l'Azienda Ospedaliero-Universitaria Policlinico – Vittorio Emanuele tutela la persona in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Regolamento (UE) 2016/679 ("GDPR"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
Scopo del presente documento è garantire che i dati personali siano trattati all'interno dell'Azienda in modo lecito, corretto e trasparente nei confronti dell'interessato, nonché secondo i principi di limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, di cui all'articolo 5 del GDPR.
La protezione delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale riconosciuto dalla Unione Europea e a tal fine l'Azienda mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente alla normativa vigente, tenuto conto della relativa natura, ambito di applicazione, contesto e finalità di trattamento, e possibile rischio di lesione dei diritti e delle libertà degli interessati.

Art. 2 - Principi applicabili al trattamento dei dati personali

Ai sensi di quanto previsto dall'art. 5 del GDPR i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

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

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

Art. 3 - Liceità del trattamento

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

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

Art. 4 - Dati trattati

L'Azienda tratta dati personali relativi a:

- utenti, assistiti, pazienti e loro familiari e/o accompagnatori;
- personale sanitario, amministrativo, tecnico e professionale della dirigenza e del comparto con rapporto di dipendenza, convenzione o collaborazione;
- personale universitario che svolge attività assistenziale, di ricerca e di didattica all'interno dell'Azienda;
- soggetti che per motivi di studio, tirocinio, stage o volontariato frequentano le strutture dell'Azienda ed effettuano trattamento di dati personali, quali specializzandi, allievi tirocinanti, volontari, ecc;
- soggetti che intrattengono rapporti contrattuali con l'Azienda ai fini della fornitura di beni e servizi, attività di assistenza o consulenza, esecuzione di opere edilizie, interventi di manutenzione su software o dispositivi medici, ecc;
- soggetti e imprese partecipanti a bandi di gara o di pubblico concorso.

L'Azienda effettua il trattamento dei soli dati necessari per le finalità per le quali vengono raccolti o trattati tra cui:

- dati personali comuni quali: nome, cognome, residenza, cittadinanza, recapito telefonico, codice fiscale, ecc;
- categorie particolari di dati personali (art. 9 del GDPR);

- dati economici quali: retribuzione, compensi, benefici, agevolazioni, ecc;
- dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR).
- dati relativi ai familiari, quando richiesti da un presupposto di legge o di regolamento.

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;
- presso enti del SSN, presso altri enti e amministrazioni pubbliche o terzi, presso pubblici registri o presso altri esercenti le professioni sanitarie.

Art. 5 - Operazioni di trattamento

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

- la raccolta dei dati;
- la registrazione dei dati, ovvero il loro inserimento su supporti, automatizzati o manuali, al fine di rendere i dati disponibili per successivi trattamenti;
- l'organizzazione dei dati, cioè il processo di lavorazione finalizzato a favorirne la fruibilità attraverso l'aggregazione, la disaggregazione, l'accorpamento, la catalogazione, ecc.;
- la conservazione dei dati;
- l'adattamento o la modifica in relazione a variazioni o a nuove acquisizioni;
- l'estrazione;
- la consultazione;
- l'uso;
- la comunicazione dei dati mediante trasmissione ad uno o più soggetti determinati, in qualunque forma, anche mediante messa a disposizione o consultazione; la comunicazione dei dati avviene solo nei casi previsti da norme di legge o regolamento;
- la comunicazione dei dati mediante diffusione, ovvero il dare conoscenza dei dati personali a soggetti indeterminati (es. pubblicazione nell'albo pretorio, ecc);
- la limitazione, cioè il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- la cancellazione;
- la distruzione.

Le operazioni di trattamento possono essere effettuate solo dal titolare, dai responsabili esterni e dai soggetti designati ed incaricati del trattamento dei dati. Non è consentito il trattamento da parte di persone non autorizzate.

Il responsabile della protezione dei dati provvede, in collaborazione con i responsabili esterni del trattamento e con i soggetti designati ed incaricati, al censimento ed aggiornamento di tutti i trattamenti di dati personali effettuati per conto del titolare del trattamento.

E' compito dei responsabili del trattamento e dei soggetti designati/incaricati effettuare la valutazione periodica della non eccedenza dei dati trattati.

Art. 6 - Le finalità e le basi giuridiche del trattamento

Il trattamento dei dati personali è effettuato dall'Azienda, in qualità di soggetto pubblico del Servizio Sanitario Nazionale, ed è consentito solo per lo svolgimento delle funzioni istituzionali assegnate nell'ambito dell'assistenza, didattica e ricerca e, pertanto, per le finalità di seguito richiamate:

Finalità del trattamento	Categorie di dati personali	Base giuridica del trattamento
Finalità di cura: erogazione di prestazioni di medicina preventiva, di diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali. Comprende le prestazioni sanitarie, sia istituzionali che in libera professione, erogate in regime di ricovero, ordinario o diurno, di assistenza specialistica ambulatoriale, di Day Service o altre modalità assistenziali, quali quelle di telemedicina o teleconsulto.	Dati personali, categorie particolari di dati personali (tra cui: dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)	**Art. 9, par. 2, lett. h) del GDPR** "Il trattamento è necessario per finalità di medicina preventiva, di diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali". **Art. 9, par. 3 del GDPR** "I dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza". **Art. 75 del D. Lgs. 196/2003**
Attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza e terapia sanitaria, ivi incluse quelle correlate ai trapianti d'organo e tessuti nonché alle trasfusioni di sangue umano	Dati personali, categorie particolari di dati personali (tra cui: dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)	**Art. 6, par. 1, lett. c) del GDPR** "Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" **Art. 6, par. 1, lett. e) del GDPR** "Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico di cui è investito il titolare del trattamento" Per i dati particolari: **Art. 9, par. 2, lett. g) del GDPR e art. 2-sexies, comma 2, lett. t) D. Lgs. 196/2003)** "Il trattamento è necessario per motivi di interesse pubblico rilevante"
Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria anche con riferimento agli aspetti di qualità e sicurezza delle prestazioni erogate	Dati personali, categorie particolari di dati personali (tra cui: dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)	**Art. 6, par. 1, lett. c) del GDPR** "Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" **Art. 6, par. 1, lett. e) del GDPR** "Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico di cui è investito il titolare del trattamento" Per i dati particolari: **Art. 9, par. 2, lett. g) e i) del GDPR e art. 2-sexies, comma 2, lett. v) D. Lgs. 196/2003)** "Il trattamento è necessario per motivi di interesse pubblico rilevante" e per "motivi di interesse pubblico nel settore della sanità pubblica"
Ricerca scientifica in campo medico, biomedico ed epidemiologico, ricerca scientifica nell'ambito di sperimentazioni cliniche sui medicinali ad uso umano	Dati personali, categorie particolari di dati personali (tra cui: dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)	**Art. 9, par. 2, lett. a) del GDPR** "L'interessato ha prestato il proprio consenso esplicito per una o più finalità specifiche" **Art. 9, par. 2, lett. i) e j) del GDPR** "Il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica" e "ai fini di ricerca scientifica o storica o a fini statistici" **Art. 110 D. Lgs. 196/2003**

Finalità del trattamento	Categorie di dati personali	Base giuridica del trattamento
Attività di didattica e formazione universitaria	Dati personali, categorie particolari di dati personali (tra cui: dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)	**Art. 9, par. 2, lett. g) del GDPR e art. 2-sexies, comma 2, lett. bb) D. Lgs. 196/2003)** "Il trattamento è necessario per motivi di interesse pubblico rilevante"
Vigilanza sulle sperimentazioni, farmacovigilanza e vigilanza sui dispositivi medici	Dati personali, categorie particolari di dati personali (tra cui: dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)	**Art. 9, par. 2, lett. g) e i) del GDPR e art. 2-sexies, comma 2, lett. z) D. Lgs. 196/2003)** "Il trattamento è necessario per motivi di interesse pubblico rilevante" e per "motivi di interesse pubblico nel settore della sanità pubblica"
Funzionamento del Registro Tumori	Dati personali, categorie particolari di dati personali (tra cui: dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)	**Art. 9, par. 2, lett. g) del GDPR, art. 2-sexies, comma 2, lett. t) e u) e art. 110 D. Lgs. 196/2003** "Il trattamento è necessario per motivi di interesse pubblico rilevante"
Instaurazione, gestione ed estinzione di rapporti di lavoro in ambito pubblico, anche non retribuito, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, pari opportunità, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici, dati biometrici, appartenenza sindacale, convinzioni religiose), dati giudiziari, relativi a carichi pendenti e condanne penali e civili per danno all'immagine o per responsabilità professionale e condanne per danno erariale nonché sanzioni disciplinari	**Art. 6, par. 1, lett. b) GDPR** "Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte" **Art. 6, par. 1, lett. c) GDPR** "Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" **Art. 88 del GDPR** Per i dati particolari: **Art. 9, par. 2, lett. g) e h) del GDPR e art. 2-sexies, comma 2, lett. u) e dd) e D. Lgs. 196/2003** "Il trattamento è necessario per motivi di interesse pubblico rilevante" e per "finalità di medicina del lavoro, valutazione della capacità lavorativa del lavoratore"
Gestione del contenzioso	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	**Art. 9, par. 2, lett. f) del GDPR** "Il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria"
Fornitura di beni e servizi o esecuzione di opere edilizie e interventi di manutenzione necessari per il perseguimento delle finalità istituzionali dell'Azienda	Dati personali	**Art. 6, par. 1, lett. b) del GDPR** "Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte"
Pubblicazione di atti e documenti per finalità di trasparenza	Dati personali	**Art. 6, par. 1, lett. e) del GDPR** "Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico di cui è investito il titolare del trattamento" **Art. 86 del GDPR**
Invio di referti online su richiesta dell'interessato	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	**Art. 9, par. 2, lett. a) del GDPR** "L'interessato ha prestato il proprio consenso esplicito per una o più finalità specifiche"
Alimentazione del Fascicolo Sanitario Elettronico	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	**Art. 9, par. 2, lett. a) del GDPR** "L'interessato ha prestato il proprio consenso esplicito per una o più finalità specifiche"
Utilizzo di app mediche con possibile accesso da parte di soggetti autorizzati esterni all'Azienda	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	**Art. 9, par. 2, lett. a) del GDPR** "L'interessato ha prestato il proprio consenso esplicito per una o più finalità specifiche"

Finalità del trattamento	Categorie di dati personali	Base giuridica del trattamento
Tutela dei beni aziendali e del patrimonio, sicurezza e incolumità delle persone, accertamento dei reati	Dati personali (immagini di videosorveglianza)	**Art. 6, par. 1, lett. e) del GDPR** "Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico di cui è investito il titolare del trattamento" **Art. 6, par. 1, lett. f) del GDPR** "Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento, o di terzi"
Analisi di gradimento e valutazione della qualità dei servizi	Dati personali	**Art. 6, par. 1, lett. a) del GDPR** "L'interessato ha prestato il proprio consenso esplicito per una o più finalità specifiche"

I trattamenti di dati personali e particolari per la rilevazione delle malattie mentali, delle malattie infettive e diffusive, della sieropositività, a fini di indagini epidemiologiche, a fini di trapianto di organi e tessuti, ai fini della tenuta del Registro Tumori, a fini di campagne di screening, ai fini del monitoraggio della spesa sanitaria, vengono effettuati nei casi e con i limiti previsti dalle normative settoriali vigenti.
L'Azienda assicura il diritto all'anonimato dell'interessato o l'adozione di misure capaci di garantire un maggior grado di tutela della riservatezza nel trattamento dei suoi dati specificatamente previsti dalle normative vigenti.
Il trattamento dei dati personali per fini di ricerca viene effettuato con il consenso dell'interessato, laddove richiesto, o, negli altri casi previsti dalla normativa vigente, previa specifica informativa ed adozione di apposite ed adeguate misure di sicurezza.
I risultati della ricerca scientifica pubblicati o comunque resi noti non possono in alcun caso contenere dati personali che rendano identificabili i soggetti ai quali si riferiscono.

Art. 7 - Categorie particolari di dati personali

L'attività dell'Azienda nell'ambito dell'assistenza sanitaria comporta il trattamento di dati appartenenti alle categorie particolari di cui all'articolo 9 del GDPR, tra cui dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il trattamento di tali dati è consentito qualora si verifichi uno dei casi riportati al paragrafo 2 del medesimo articolo 9 che di seguito si richiama:

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 [.....];*
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 è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali […];*
e) *il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;*
f) *il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;*
g) *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;*
h) *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;

i) 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;

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

In conformità a quanto previsto dall'art. 2-sexies, comma 1, del D. Lgs. 196/2003, i trattamenti delle categorie particolari di dati personali, necessari per motivi di interesse pubblico rilevante ai sensi dell'art. 9, paragrafo 2, lettera g) del GDPR, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Il medesimo articolo, individua i motivi di interesse pubblico rilevante che consentono il trattamento di categorie particolari di dati personali.
I dati particolari sono trattati dall'Azienda qualora essenziali e necessari allo svolgimento delle attività istituzionali ad essa assegnate e nel caso in cui tali attività non possano essere adempiute mediante il trattamento di dati anonimi o di dati personali di diversa natura.
Per il trattamento dei dati genetici si fa, inoltre, rinvio alle prescrizioni del Garante per la protezione dei dati personali (provvedimento n. 146 del 5 giugno 2019), nonché alle misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute previste dall'art. 2-septies del D. Lgs. 196/2003.

Art. 8 - Il trattamento dei dati dei lavoratori

L'Azienda tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, d'instaurazione, gestione ed estinzione di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.
Il trattamento delle categorie particolari di dati personali è effettuato solo se necessario:

a) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa dell'Unione europea, da leggi, da regolamenti o da contratti collettivi anche aziendali, ai sensi del diritto interno, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro (art. 88 del Regolamento UE 2016/679), nonché del riconoscimento di agevolazioni ovvero dell'erogazione di contributi, dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro, nonché in materia fiscale e sindacale;
b) anche fuori dei casi di cui alla lettera a), in conformità alla legge e per scopi determinati e legittimi, ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori;
c) per perseguire finalità di salvaguardia della vita o dell'incolumità fisica del lavoratore o di un terzo;

d) per far valere o difendere un diritto, anche da parte di un terzo, in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione, nei casi previsti dalle leggi, dalla normativa dell'Unione europea, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose; resta salvo quanto stabilito dall'art. 60 del Codice;
e) per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di salute e sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale;
f) per garantire le pari opportunità nel lavoro;
g) per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro.

L'Azienda adotta le massime cautele nel trattamento dei dati personali dei dipendenti idonei a rivelare lo stato di salute, le abitudini sessuali, l'origine razziale ed etnica, le convinzioni politiche o d'altro genere.

I dati che rivelano le convinzioni religiose o filosofiche ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico sono trattati esclusivamente in caso di fruizione di permessi in occasione di festività religiose o per le modalità di erogazione dei servizi di mensa o, nei casi previsti dalla legge, per l'esercizio dell'obiezione di coscienza.

I dati che rivelano le opinioni politiche o l'appartenenza sindacale, o l'esercizio di funzioni pubbliche e incarichi politici, di attività o di incarichi sindacali sono trattati esclusivamente ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali, nonché per consentire l'esercizio dei diritti sindacali compreso il trattamento dei dati inerenti alle trattenute per il versamento delle quote di iscrizione ad associazioni od organizzazioni sindacali.

In caso di partecipazione dei dipendenti ad operazioni elettorali in qualità di rappresentanti di lista, in applicazione del principio di necessità, nella documentazione da presentare al fine del riconoscimento di benefici di legge, non devono essere e trattati dati che rivelino le opinioni politiche (ad esempio, non deve essere richiesto il documento che designa il rappresentate di lista essendo allo scopo sufficiente la certificazione del presidente di seggio).

I dati genetici non possono essere trattati al fine di stabilire l'idoneità professionale di un candidato all'impiego o di un lavoratore, neppure con il consenso dell'interessato.

In tutte le comunicazioni all'interessato che contengono categorie particolari di dati, devono essere utilizzate forme di comunicazione anche elettroniche individualizzate nei confronti di quest'ultimo o di un suo delegato, anche per il tramite di personale autorizzato. Nel caso in cui si proceda alla trasmissione del documento cartaceo, questo dovrà essere trasmesso, di regola, in plico chiuso, salva la necessità di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto.

I documenti che contengono dati categorie particolari di dati, ove debbano essere trasmesse ad altri uffici o funzioni in ragione delle rispettive competenze, devono contenere esclusivamente le informazioni necessarie allo svolgimento della funzione senza allegare, ove non strettamente indispensabile, documentazione integrale o riportare stralci all'interno del testo. A tal fine dovranno essere selezionate e impiegate modalità di trasmissione della documentazione che ne garantiscano la ricezione e il relativo trattamento da parte dei soli uffici o strutture organizzative competenti e del solo personale autorizzato.

Nella predisposizione dei turni di servizio, qualora occorra mettere a disposizione di soggetti diversi dall'interessato (ad es. altri colleghi) i dati relativi alle presenze ed assenze dal servizio, la documentazione non deve contenere, nemmeno attraverso acronimi o sigle, le causali dell'assenza dalle quali sia possibile evincere la conoscibilità di particolari categorie di dati personali (es. permessi sindacali o dati sanitari).

La pubblicazione delle graduatorie per la selezione di personale o per la concessione di benefici economici, agevolazioni o contributi, viene effettuata dopo avere verificato che le informazioni ivi contenute non comportino la divulgazione di dati personali non necessari, né 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 applica quanto previsto dalla Delibera del Garante per la protezione dei dati personali del 14/06/2007 riguardante le linee guida in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, nonché le prescrizioni del Garante contenute nel provvedimento n. 146 del 5 giugno 2019.

Art. 9 - Il trattamento per finalità di ricerca medica, biomedica ed epidemiologica

Il trattamento ai fini di ricerca scientifica è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, così come richiamato all'articolo 89, paragrafo 1, del GDPR, volte a garantire il rispetto del principio della minimizzazione dei dati.
Nei trattamenti per finalità di ricerca scientifica l'Azienda applica le prescrizioni del Garante per la protezione dei dati personali e assicura la diffusione e il rispetto delle regole deontologiche di cui all'allegato A.4 del D. Lgs. n. 196/2003 fra tutti coloro che sono coinvolti nel trattamento dei dati personali realizzato nell'ambito delle attività di ricerca; segnala, inoltre, al Garante le violazioni delle regole deontologiche di cui viene a conoscenza.
Ai sensi di quanto previsto dall'art. 110 del D. Lgs. 196/2003, così come modificato dal D. Lgs. n. 101/2018, il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o regolamento o al diritto dell'Unione Europea in conformità all'articolo 9, paragrafo 2, lettera j), del GDPR, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del D.Lgs. 502/92, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del GDPR. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di ricerca. In tali casi il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del GDPR.
In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 16 del GDPR nei riguardi dei trattamenti per finalità di ricerca medica, scientifica ed epidemiologica, l'aggiornamento, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.
In caso di trattamento ulteriore da parte di soggetti terzi dei dati personali a fini di ricerca scientifica o a fini statistici, si applicano le disposizioni contenute nell'art. 110-bis del D.Lgs. 196/2003.

Art. 10 - Il trattamento dei dati nell'ambito del Registro Tumori

Il Registro Tumori integrato per le province di Catania, Messina e Enna, facente capo all'Azienda, effettua il trattamento di dati personali per finalità di interesse pubblico rilevante di cui all'art. 2-sexies, comma 2, del D. Lgs. n. 196/2003, e per finalità di ricerca medica, biomedica ed epidemiologica di cui all'art. 110 del D. Lgs. n. 196/2003. Nell'ambito di tali finalità il Registro Tumori è finalizzato a:

- produrre misure dell'incidenza, mortalità, sopravvivenza e prevalenza dei tumori;

- descrivere il rischio della malattia per sede e per tipo di tumore, età, genere ed ogni altra variabile di interesse per la ricerca scientifica;
- svolgere studi epidemiologici sugli andamenti temporali e la distribuzione territoriale dei casi, sui fattori di rischio dei tumori, sugli esiti degli interventi di diagnosi precoce, delle terapie e dei percorsi diagnostico-terapeutici, anche in collaborazione con altri enti e strutture regionali, nazionali ed internazionali di ricerca scientifica in campo epidemiologico;
- produrre dati anonimi e aggregati per la programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, inerente gli interventi di prevenzione primaria e secondaria rivolti alle persone ed all'ambiente di vita e lavoro, nonché dell'efficacia dei programmi di screening;
- monitorare e valutare i dati relativi all'appropriatezza e qualità dei servizi diagnostici terapeutici, alla sopravvivenza dei pazienti affetti da cancro.

Per il funzionamento del Registro Tumori si rinvia a quanto contenuto nel regolamento adottato dalla Regione Sicilia.

Art. 11 - Periodo di conservazione dei dati personali

I dati personali saranno conservati solo per il tempo necessario ad adempiere alle finalità per le quali sono stati raccolti, nel rispetto del principio di minimizzazione di cui all’articolo 5, comma 1, lettera c) del GDPR nonché degli obblighi di legge cui è tenuto il Titolare.
Con particolare riferimento alla documentazione sanitaria ed amministrativa, l’Azienda è tenuta al rispetto dei tempi di conservazione previsti dal vigente ordinamento giuridico.
Con distinti provvedimenti l’Azienda definisce e aggiorna periodicamente il Regolamento per la conservazione e lo scarto dei documenti di archivio in conformità a quanto contemplato dall’Amministrazione Archivistica statale attraverso i competenti Organi del Ministero per i Beni e le Attività Culturali.
L’Azienda assicura l’adozione di apposite misure e procedure attraverso le quali:

- procede alla distruzione dei dati personali, secondo le modalità previste dalla legge, una volta terminato il limite minimo di conservazione dei documenti analogici e digitali e dei dati personali ivi riportati;
- smaltisce gli apparati hardware o supporti rimovibili di memoria con modalità che non rendono possibile accedere ad alcun dato personale di cui è titolare l’Azienda;
- procede al riutilizzo degli apparati di memoria o hardware con modalità tali da assicurare che non sia possibile accedere ad alcun dato personale di cui è titolare l’Azienda.

Art. 12 - Categorie di destinatari

I dati personali oggetto di trattamento saranno comunicati esclusivamente ai soggetti autorizzati ed ai responsabili del trattamento allo scopo designati dal titolare del trattamento.
I dati personali, inclusi quelli particolari e giudiziari (art. 9 e 10 del GDPR), potranno essere comunicati ad altro soggetto pubblico o a terzi quando ciò sia previsto da una norma di legge o di regolamento o nel caso risulti necessario per lo svolgimento delle funzioni istituzionali assegnate all’Azienda o per le finalità per le quali i dati sono stati raccolti e trattati.
Al di fuori dei casi previsti da una norma di legge o di regolamento, i dati personali potranno essere comunicati solo previo consenso esplicito dell’interessato.
Si riportano di seguito le principali categorie di destinatari cui possono essere comunicati i dati personali nei casi previsti da norme di legge o di regolamento:

Finalità del trattamento	Categorie di dati personali	Categorie di destinatari
Finalità di cura, Attività amministrative e certificatorie	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	• Medico di Medicina Generale o Pediatra di Libera Scelta • Azienda Sanitaria di residenza • Regione Siciliana - Assessorato della Salute • Ministero della Salute (flussi ministeriali) • Ministero dell'Economia - SOGEI • Agenzia Italiana del Farmaco • Forze dell'Ordine o Autorità Giudiziaria • Ogni altro soggetto se previsto da norma di legge o di regolamento
Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria anche con riferimento agli aspetti di qualità e sicurezza delle prestazioni erogate	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	• Regione Siciliana - Assessorato della Salute • Ministero della Salute • AGENAS • Ogni altro soggetto se previsto da norma di legge o di regolamento
Ricerca scientifica in campo medico, biomedico ed epidemiologico, ricerca scientifica nell'ambito di sperimentazioni cliniche sui medicinali ad uso umano	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	• Enti e istituti di ricerca • Ministero della Salute • AGENAS • Ogni altro soggetto indicato nell'informativa • Paese estero (se previsto nel protocollo di ricerca) Vengono applicate misure di pseudonimizzazione laddove compatibile con le finalità del trattamento. Pubblicazione di soli dati anonimi e in forma aggregata o con altre modalità che assicurino la non identificabilità.
Attività di didattica e formazione universitaria	Dati personali, categorie particolari di dati personali	Nessun destinatario individuato
Vigilanza sulle sperimentazioni, farmacovigilanza e vigilanza sui dispositivi medici	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	• Ministero della Salute • Agenzia Italiana del Farmaco • Ogni altro soggetto se previsto da norma di legge o di regolamento
Funzionamento del Registro Tumori	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	• Titolari del trattamento dei dati dei Registri Tumori di altre Regioni, previa stipula di convenzione. • Università, Enti e istituti di ricerca e società scientifiche per lo svolgimento di studi in campo medico, biomedico ed epidemiologico.
Instaurazione, gestione ed estinzione di rapporti di lavoro, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, pari opportunità, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici), dati giudiziari, relativi a carichi pendenti e condanne penali e civili per danno all' immagine o per responsabilità professionale e condanne per danno erariale, nonché sanzioni disciplinari	• Regione Siciliana - Assessorato della Salute, Ispettorato del Lavoro • Ministero della Salute • Ministero dell'Economia – Agenzia delle Entrate • Ministero per la Pubblica Amministrazione • INPS • INAIL • ANAC • Istituto Tesoriere dell'Azienda • Azienda sanitaria di residenza • Collegi Medici competenti • ISTAT • ARAN • Enti previdenziali e assicurativi • Autorità Giudiziaria e Forze dell'Ordine • Corte dei Conti • Ogni altro soggetto se previsto da norme di legge o di regolamento

Finalità del trattamento	Categorie di dati personali	Categorie di destinatari
Gestione del contenzioso	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	• Autorità Giudiziaria • Professionista incaricato di assistenza legale • Consulente tecnico d'ufficio o di parte • Ogni altro soggetto se previsto da norme di legge o di regolamento
Fornitura di beni e servizi o esecuzione di opere edilizie e interventi di manutenzione necessari per il perseguimento delle finalità istituzionali dell'Azienda	Dati personali	• Regione Siciliana - Assessorato della Salute, Centrale Unica di Committenza • ANAC • MEPA – CONSIP • Ogni altro soggetto se previsto da norme di legge o di regolamento
Pubblicazione di atti e documenti per finalità di trasparenza o pubblicità legale	Dati personali	In presenza di un obbligo normativo in materia di trasparenza, la pubblicazione sul sito web aziendale viene effettuata previo oscuramento od omissione dei dati personali non pertinenti o non indispensabili rispetto alle finalità di trasparenza o pubblicità.
Invio di referti online su richiesta dell'interessato	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	Interessato e soggetti autorizzati dall'interessato
Alimentazione del Fascicolo Sanitario Elettronico	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	Interessato e soggetti autorizzati dall'interessato
Utilizzo di app mediche con possibile accesso da parte di soggetti autorizzati esterni all'Azienda	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	Interessato e soggetti autorizzati dall'interessato
Tutela dei beni aziendali e del patrimonio, sicurezza e incolumità delle persone, accertamento dei reati	Dati personali (immagini di videosorveglianza)	Autorità Giudiziaria e Forze dell'Ordine nei casi previsti dalla legge
Analisi di gradimento e valutazione della qualità dei servizi	Dati personali	Possono essere comunicati e diffusi solo dati anonimi in forma aggregata

Art. 13 - Comunicazione dei dati all'interessato

I dati personali particolari (art. 9 GDPR) possono essere resi noti all'interessato, oltre che mediante consegna diretta allo stesso, anche attraverso modalità telematiche nei casi e nei modi previsti dalla specifica normativa e su consenso specifico dell'interessato.
La documentazione sanitaria viene consegnata in busta chiusa e può essere ritirata dall'interessato o da persona diversa da questi delegata, salvo il caso di documenti contenenti dati regolati da normative speciali che prevedono il ritiro esclusivamente da parte della persona cui tali documenti sono riferiti (ad esempio referti HIV).

Art. 14 - Accesso ai documenti amministrativi, accesso civico, accesso generalizzato

L'Azienda applica quanto contenuto nell'art. 59 del D. Lgs. 196/2003 in materia di accesso a documenti amministrativi contenenti dati personali, disciplinato dalla L. 241/90, e di accesso civico, disciplinato dal D. Lgs. 33/2013. In osservanza delle richiamate disposizioni l'Azienda valuta caso per caso, anche con riguardo ad altre regolamentazioni specifiche, la possibilità da parte di terzi di accedere a documenti contenenti dati di cui agli articoli 9 e 10 del GDPR.

Ai sensi dell'art. 60 del D. Lgs. 196/2003, quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.
Si rinvia per gli ulteriori aspetti al Regolamento aziendale per il diritto di accesso agli atti, ai dati e ai documenti (deliberazione n. 1073 del 5/7/2017).

Art. 15 - Accesso alle cartelle cliniche

Come disposto dall'art. 92, comma 2, del D. Lgs. 196/2003, 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 GDPR, 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. 16 - 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. L'Azienda applica, altresì, quanto previsto dall'articolo 109 del D. Lgs. 196/2003 in merito all'osservanza delle disposizioni e modalità tecniche per la rilevazione dei dati statistici relativi agli eventi nascita e per i flussi di dati.
In caso di madre che abbia dichiarato di non voler essere nominata si applicano le disposizioni di cui all'art. 93, commi 2 e 3, del D. Lgs. 196/2003.

Art. 17 - La pubblicazione di dati per finalità di trasparenza

Ai sensi dell'art. 2-septies, comma 8, del D. Lgs. n. 196/2003, e dell'art. 7-bis, comma 6, del D. Lgs. n. 33/2013 è sempre vietata la diffusione di dati genetici, biometrici e relativi alla salute e alla vita sessuale.
Salvo diversa disposizione di legge, i documenti da pubblicare sul sito istituzionale per finalità di trasparenza e/o pubblicità legale non devono contenere in forma intelligibile dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle finalità di trasparenza della pubblicazione.
Tra i dati da oscurare o rendere anonimi o da pseudonomizzare si citano, a titolo esemplificativo e non esaustivo: utenza telefonica e posta elettronica privati, indirizzi di residenza, codice fiscale, indicatore ISEE, carta d'identità o altra documentazione personale, numero di IBAN, dati relativi a condanne penali o reati, documentazione da cui si possa desumere, anche indirettamente, l'esistenza di patologie o condizioni di invalidità, disabilità, handicap fisici e/o psichici che riguardano l'interessato o familiari, documentazione da cui si evinca l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, politico o sindacale. In tutti questi casi l'ufficio competente alla redazione e conservazione del documento, con la consulenza ove necessario del Responsabile della protezione dei dati, verifica, caso per caso, se esistano i presupposti per oscurare od omettere determinate informazioni prima della trasmissione all'ufficio deputato alla pubblicazione sul sito web aziendale.

Per assicurare la completezza dell'atto amministrativo, i dati personali da escludere dalla pubblicazione sono mantenuti nell'originale integrale del documento a disposizione degli uffici competenti e del personale autorizzato.
Si fa rinvio alle indicazioni contenute nelle linee guida del Garante per la protezione dei dati personali (provvedimento n. 243 del 15/05/2014 "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati").
Effettuata la previa valutazione circa i presupposti e l'indispensabilità della pubblicazione delle particolari categorie di dati personali e dei dati relativi a condanne penali o reati (art. 9 e 10 del GDPR), devono essere adottate misure e accorgimenti tecnici volti ad evitare l'indicizzazione e la rintracciabilità tramite i motori di ricerca ed il loro riutilizzo.
I dati personali pubblicati nella sezione "Amministrazione Trasparente" del sito web aziendale sono riutilizzabili solo alle condizioni previste dalla normativa vigente sul riuso dei dati pubblici (direttiva comunitaria 2003/98/CE e D. Lgs. 36/2006 di recepimento della stessa), in termini compatibili con gli scopi originari del trattamento (art. 5, par. 1, lett. b) del GDPR).

Parte seconda – Diritti dell'interessato

Art. 18 - Informazioni sul trattamento

L'Azienda, quale titolare del trattamento, adotta misure appropriate per fornire all'interessato tutte le informazioni e comunicazioni riguardanti il trattamento dei dati in forma concisa, trasparente intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni rivolte specificatamente ai minori.
Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
L'Azienda a tal riguardo predispone specifiche informative sul trattamento dei dati personali che riportano le seguenti informazioni previste dalla vigente normativa (art. 13 e 14 del GDPR):

a) l'identità e i dati di contatto del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
c) i legittimi interessi perseguiti dal titolare del trattamento o da terzi (nel caso di trattamenti basati sull'art. 6, par. 1, lettera f) del GDPR);
d) gli eventuali destinatari, o categorie di destinatari, cui possono essere comunicati i dati;
e) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
f) 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 o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
g) qualora la liceità del trattamento dei dati sia basata sul preventivo rilascio del consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
h) il diritto di proporre reclamo all'Autorità Garante per la Protezione dei dati personali;
i) 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;

j) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
k) nel caso in cui i dati personali non siano stati ottenuti presso l'interessato, le categorie di dati personali in questione, la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

L'informativa all'interessato viene fornita per iscritto, anche per estratto, tramite materiale informativo reso disponibile nei luoghi comuni dell'Azienda e presso la sezione "Tutela della privacy" del portale web aziendale www.policlinicovittorioemanuele.it.
Sono altresì predisposte specifiche informative per:

- trattamento dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente o con contratto di collaborazione/consulenza;
- trattamento dei dati per la partecipazione a procedure concorsuali e nei casi di ricezione di curriculum spontaneamente trasmessi dall'interessato (art. 111-bis D. Lgs. 196/2003);
- trattamento dei dati per fornitori di beni e servizi
- trattamento dei dati per videosorveglianza.

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.

Art. 19 - Il consenso al trattamento dei dati

Ai sensi di quanto previsto dal Provvedimento n. 55/2019 del Garante per la protezione dei dati personali, nel caso di trattamenti per "finalità di cura", effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza, non è richiesto il consenso del paziente per i trattamenti necessari alla prestazione sanitaria richiesta dall'interessato, indipendentemente dalla circostanza che operi in qualità di libero professionista (presso uno studio medico) ovvero all'interno di una struttura sanitaria pubblica o privata.
Sono da intendersi necessari alla prestazione sanitaria richiesta dall'interessato, i trattamenti connessi alle attività amministrativo/contabili che l'Azienda, ai sensi di disposizioni di legge o di regolamento, è tenuta ad effettuare in qualità di soggetto pubblico operante nell'ambito del Servizio Sanitario Regionale.
Qualora sia richiesto il consenso dell'interessato, lo stesso deve essere reso mediante sottoscrizione di apposita modulistica in uso presso le Unità Operative, previa visione e presa d'atto dell'informativa.
L'eventuale rifiuto a prestare il consenso al trattamento dei dati per finalità diverse da quelle di cura, comporta l'impossibilità di effettuare il relativo trattamento dei dati.
Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

L’interessato ha il diritto di revocare il proprio consenso al trattamento dei dati personali in qualsiasi momento e ciò non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò.
La manifestazione del consenso sarà valida ed efficace fino alla revoca dello stesso o, per i minorenni, fino al compimento del diciottesimo anno d’età. Il consenso è revocato con la stessa facilità con cui è accordato.
Qualora il trattamento dei dati personali sia basato sul rilascio del preventivo consenso da parte dell’interessato, è compito dell’Azienda dimostrare che questi abbia prestato il proprio consenso libero e informato al trattamento dei dati personali.
Il Titolare assicura attraverso idonee modalità l’archiviazione dei consensi espressi dagli interessati in modo da rendere fruibili e rintracciabili le autorizzazioni da questi rilasciate.
Il consenso al trattamento dei dati è comunque distinto dal consenso informato all’atto sanitario di cui alla Procedura PGS-UOQ-7-02.

Art. 20 - Diritto di accesso

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 GDPR):

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo al Garante della protezione dei dati;
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, e, 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 dei dati personali non deve ledere i diritti e le libertà altrui.

Art. 21 - 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 (art. 16 GDPR). 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. 22 - Diritto di cancellazione

Ai sensi dell'art. 17 del GDPR 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.

L'esercizio di tale diritto in ambito sanitario va rapportato agli obblighi di conservazione documentale previsti dalla legge ed ai motivi di esclusione richiamati all'art. 17, paragrafo 3, del GDPR.

Art. 23 - Diritto di limitazione di trattamento

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle ipotesi richiamate dall'art. 18, paragrafo 1, del GDPR.
Se il trattamento è limitato, i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante.
L'interessato che ha ottenuto la limitazione del trattamento è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Art. 24 - 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. 25 - Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano, per le situazioni richiamate all'art. 21 del GDPR, 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 riguarda, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

Art. 26 - Reclamo al Garante

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il GDPR ha il diritto di proporre reclamo al Garante per la protezione dei dati personali ai sensi dell'articolo 77 del GDPR.

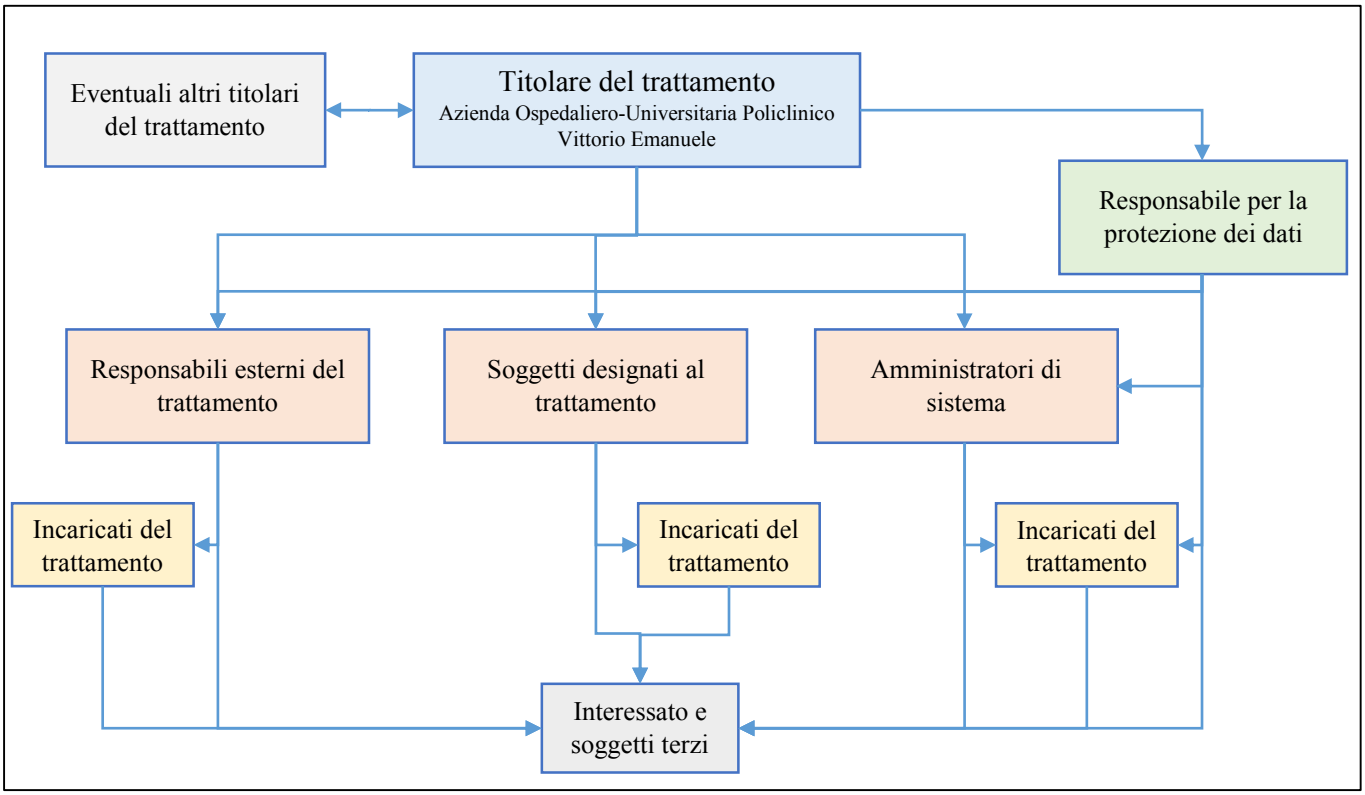
Art. 27 - Diritti riguardanti le persone decedute

Ai sensi di quanto previsto dall’art. 2-terdecies del D. Lgs. 196/2003, i diritti di cui agli articoli da 15 a 22 del GDPR, riferiti a dati personali concernenti persone decedute, possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

Parte terza – Soggetti del trattamento

Art. 28 - Soggetti coinvolti

Il trattamento dei dati comporta il coinvolgimento dei soggetti indicati nel successivo organigramma, con svolgimento delle attività e compiti descritti nei successivi articoli.



Art. 29 - Il titolare del trattamento

Il titolare del trattamento dei dati personali è la persona fisica o giuridica, l’Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Ai sensi e per gli effetti del GDPR, titolare del trattamento dei dati personali è l'**Azienda Ospedaliero-Universitaria "Policlinico – Vittorio Emanuele"**, rappresentata dal Direttore Generale, in qualità di rappresentante legale della stessa, con sede a Catania in Via S. Sofia n. 78.
Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, quali la pseudonimizzazione e la cifratura dei dati personali, la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati. Le misure tecniche ed organizzative messe in atto dal titolare sono altresì volte a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
In aggiunta a quanto sopra, il Titolare del trattamento:

- designa il responsabile della protezione dei dati di cui all'art. 37 del GDPR;
- nomina con proprio atto i responsabili esterni del trattamento dei dati personali di cui all'art. 28 del GDPR impartendo agli stessi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, all'esercizio dei diritti dell'interessato di cui al Capo III del GDPR;
- attribuisce, nell'ambito dell'assetto organizzativo aziendale, specifici compiti e funzioni connessi al trattamento dei dati ai soggetti designati secondo quanto previsto dall'art. 2-quaterdecies, comma 1, del D. Lgs. 196/2003;
- individua le modalità più opportune per autorizzare al trattamento dei dati le persone che operano sotto la propria diretta autorità, ai sensi dell'art. 2-quaterdecies, comma 2, del D. Lgs. 196/2003;
- tiene il registro delle attività di trattamento svolte sotto la propria responsabilità secondo quanto previsto dall'art. 30 del GDPR;
- in caso di violazione dei dati personali provvede alla notifica al Garante per la protezione dei dati personali senza ingiustificato ritardo secondo le modalità e i contenuti di cui all'art. 33 del GDPR;
- svolge, nei casi previsti dall'art. 35 del GDPR, una valutazione d'impatto sulla protezione dei dati consultandosi con il responsabile della protezione dei dati e procede, qualora necessario, alla consultazione preventiva di cui all'art. 36 del GDPR.

Art. 30 - Contitolari del trattamento

Nel caso di due o più titolari di trattamento, l'Azienda determina in modo congiunto le finalità ed i mezzi del trattamento determinando, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR.

Art. 31 - Interessato e soggetti terzi

L'interessato del trattamento è la persona fisica cui si riferiscono i dati personali. La normativa attribuisce all'interessato l'esercizio dei diritti richiamati nella parte seconda del presente regolamento. Le modalità per l'esercizio dei diritti sono riportate nell'informativa sul trattamento dei dati messa a disposizione degli interessati.
I soggetti terzi costituiscono la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non siano l'interessato, il titolare del trattamento, il responsabile e le persone autorizzate al trattamento.

Art. 32 - Responsabili esterni del trattamento

I soggetti esterni all'Azienda cui sono affidate attività di competenza aziendale di qualunque natura (ad esempio: assistenza legale, fornitura di beni o servizi, ecc), che comportano necessariamente il trattamento di dati personali di cui l'Azienda è titolare, vengono individuati quali responsabili del trattamento qualora presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di legge e garantisca la tutela dei diritti dell'interessato.
Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento.
Il titolare del trattamento informa ciascun responsabile del trattamento dei dati delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti. I trattamenti da parte di un responsabile del trattamento sono disciplinati da atto scritto che vincola il responsabile del trattamento al titolare del trattamento e che stabilisce la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.
Il titolare del trattamento e 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, salvo che lo richieda la normativa vigente.
Il responsabile esterno del trattamento inoltre:

- tratta i dati personali solo su istruzione documentata del titolare del trattamento;
- designa, in forma scritta, i soggetti incaricati del trattamento dei dati personali che operano sotto la propria diretta autorità per il trattamento dei dati di propria competenza, e si assicura che gli stessi si attengano alle istruzioni loro impartite e si siano impegnati a mantenere la riservatezza di tali dati o abbiano un adeguato obbligo legale di riservatezza;
- adotta le misure di sicurezza richieste ai sensi dell'art. 32 del GDPR;
- verifica l'esattezza, l'aggiornamento, la pertinenza e la congruità dei dati, in rapporto all'attività svolta;
- effettua, limitatamente all'ambito e agli aspetti di competenza, l'analisi dei rischi che incombono sui trattamenti dei dati e nella conservazione dei medesimi;
- verifica periodicamente il corretto trattamento dei dati personali da parte dei soggetti incaricati del trattamento;
- segnala al Responsabile della protezione dei dati l'inizio o la cessazione di trattamenti di dati personali e della cancellazione di dati personali, al fine di permettere l'aggiornamento del registro delle attività di trattamento;
- segnala tempestivamente al titolare del trattamento , e comunque entro 24 ore dal momento in cui è venuto a conoscenza, ogni violazione dei dati personali che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati trasmessi o comunque trattati;
- svolge ogni altra funzione specificatamente riportata nell'art. 28 del GDPR, cui si rimanda per integrale riferimento, tra cui, in particolare:
    - assiste il titolare del trattamento, nella misura in cui ciò sia possibile, e tenendo conto della natura del trattamento e delle informazioni a sua disposizione, al fine di soddisfarne l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato e garantire il rispetto degli obblighi di legge;
    - mette a disposizione del titolare del trattamento le informazioni necessarie per dimostrare il rispetto degli obblighi di legge previsti dall'art. 28 del GDPR dati e contribuisce alle attività di controllo, revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un soggetto da questi incaricato

- presta ogni collaborazione con il titolare per la notifica delle violazioni all'Autorità di controllo e agli interessati.

Il Responsabile, su richiesta del titolare del trattamento, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimento innanzi all'Autorità di controllo o all'Autorità Giudiziaria per aspetti che riguardano il trattamento dei dati di propria competenza.
Le strutture interne dell'Azienda che provvedono alla stesura o validazione degli atti che disciplinano i rapporti con i soggetti esterni (contratti, convenzioni, scritture private, conferimenti, etc.), sono tenute ad inserire negli atti stessi l'indicazione che l'Azienda provvederà successivamente, ma comunque prima di iniziare le operazioni di trattamento dei dati, a designare il contraente quale responsabile del trattamento dei dati personali, e a impartire allo stesso specifiche disposizioni operative.
La nomina del Responsabile esterno avviene mediante contratto o accordo quadro, firmato da entrambe le parti, contenente gli elementi previsti dall'art. 28 par. 3, del GDPR. Gli originali sono custoditi dal titolare e copia viene trasmessa al responsabile della protezione dei dati che aggiorna l'elenco dei responsabili esterni ed effettua eventuali attività di verifica.

Art. 33 - Soggetti designati al trattamento: funzioni e compiti loro attribuiti

L'art. 2-quaterdecies, comma 1, del D. Lgs. 196/2003 conferisce al Titolare del trattamento la possibilità di prevedere che specifici compiti e funzioni connesse al trattamento dei dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità.
A tal riguardo, considerata la complessità e la molteplicità dei trattamenti connessi allo svolgimento delle funzioni istituzionali svolte dall'Azienda, il titolare del trattamento individua quali soggetti designati al trattamento, ai sensi del richiamato articolo 2-quaterdecies, comma 1, i seguenti soggetti già in precedenza individuati quali "Responsabili interni del trattamento":

- Direttore Sanitario;
- Direttore Amministrativo;
- Direttori Medici dei Presidi Ospedalieri;
- Direttori/Responsabili delle Unità Operative Complesse e delle Unità Operative Semplici Dipartimentali;
- Medici che svolgono attività libero professionale;
- Sperimentatori di studi clinici condotti in ambito aziendale;
- Responsabili dei Settori Tecnico-Amministrativi;
- Dirigenti responsabili delle Unità Operative di Staff;
- Responsabili del Servizio infermieristico.

I soggetti designati al trattamento svolgono funzioni di gestione, coordinamento e controllo delle attività di trattamento dei dati personali svolte nell'ambito della struttura di competenza.

Ai soggetti designati sono in dettaglio attribuiti i seguenti compiti e funzioni connessi al trattamento dei dati:

1. trattare i dati attenendosi alle istruzioni predisposte dal titolare del trattamento e ad ogni altra disposizione aziendale in materia di protezione dei dati personali;
2. verificare e controllare che nell'ambito del servizio di propria competenza il trattamento dei dati sia effettuato in conformità al GDPR e alle vigenti disposizioni legislative nazionali e aziendali in materia di trattamento dei dati;
3. individuare e nominare per iscritto il personale incaricato del trattamento dei dati presso la propria struttura, eventualmente specificando le tipologie di trattamento che gli stessi sono autorizzati ad effettuare;

4. fornire al personale incaricato le istruzioni predisposte dal titolare del trattamento e impartire agli stessi, se ritenuto necessario, ulteriori e specifiche disposizioni operative per il corretto trattamento dei dati, vigilando sul loro rispetto da parte degli incaricati;
5. vigilare sul rispetto degli obblighi di riservatezza e di non divulgazione dei dati personali di cui gli incaricati del trattamento vengono a conoscenza nel corso dell'attività lavorativa;
6. verificare che nella struttura di propria competenza siano adottate e rispettate tutte le misure di sicurezza tecniche ed organizzative adeguate al trattamento dei dati, con particolare riferimento alle misure volte a ridurre i rischi di distruzione o perdita dei dati, accessi non autorizzati, trattamenti non consentiti o non conformi alle finalità di trattamento, segnalando eventuali situazioni di rischio;
7. curare la diffusione, presso il personale di competenza, delle norme, delle linee guida e di ogni altra disposizione impartita dall'Azienda riguardante il trattamento dei dati personali e adottare eventuali disposizioni interne e indicazioni di comportamento per il personale, i pazienti, gli studenti, i tirocinanti e i visitatori;
8. collaborare con il responsabile della protezione dei dati per la raccolta delle informazioni relative al censimento dei trattamenti e banche dati nell'ambito della propria struttura di competenza, ai fini della redazione ed aggiornamento del registro dei trattamenti;
9. collaborare con il titolare del trattamento ed il responsabile della protezione dei dati per dimostrare il rispetto degli obblighi relativi alla protezione dei dati personali;
10. collaborare con il titolare del trattamento affinché sia garantito un corretto riscontro alle richieste pervenute dagli interessati per l'esercizio dei diritti ai sensi degli articoli da 15 a 22 del GDPR;
11. informare il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione dei dati personali (data breach).
12. svolgere ogni altra funzione specificatamente richiesta dal titolare in materia di protezione dei dati.

In aggiunta ai compiti sopra riportati ed in relazione alle funzioni di organizzazione e coordinamento attribuite, sono individuati i seguenti specifici compiti per i soggetti designati in qualità di Direttore Amministrativo, Direttore Sanitario e di Direttore Medico di Presidio Ospedaliero, relativamente ai servizi di rispettiva competenza:

1. Curare l'organizzazione ed il funzionamento operativo dei servizi di propria competenza, anche con specifico riferimento agli aspetti di protezione e sicurezza dei dati personali;
2. Promuovere, nell'ambito dei servizi di propria competenza, la messa in atto delle disposizioni normative ed aziendali per la protezione dei dati personali anche attraverso il coinvolgimento del Responsabile della protezione dei dati e dei Direttori/Responsabili delle Unità Operative interessate;
3. Sensibilizzare i servizi di propria competenza sulle tematiche legate alla protezione dei dati personali;
4. Collaborare con il titolare del trattamento ed il responsabile della protezione dei dati ai fini della protezione e sicurezza dei dati personali e segnalare agli stessi eventuali situazioni di criticità.

Art. 34 - Incaricati del trattamento

Ai sensi dell'art. 2-quaterdecies, comma 2, del D. Lgs. 196/2003, gli incaricati del trattamento costituiscono i soggetti autorizzati al trattamento dei dati. Tali figure vengono espressamente individuate dal titolare o dai soggetti designati o dai responsabili esterni del trattamento i quali forniscono loro per iscritto istruzioni operative dettagliate e specifiche sulle corrette modalità di trattamento e vigilano sul rispetto di tali istruzioni, anche attraverso verifiche periodiche.
Possono altresì essere individuati incaricati del trattamento i soggetti che a qualsiasi titolo (ad esempio: tirocinanti, studenti, stagisti, volontari, libero professionisti, borsisti, consulenti, ecc.), prestino la loro opera, anche in via temporanea, all'interno delle strutture dell'Azienda in attività che comportano il trattamento di dati personali per conto dell'Azienda. Per attività che non comportano un trattamento dei dati, è richiesto il rispetto di impegno alla riservatezza e alla non divulgazione di notizie acquisite nel corso dell'attività svolta.

Tutti i soggetti incaricati del trattamento dei dati:

- trattano i dati personali attenendosi alle istruzioni predisposte dal titolare del trattamento, nonché alle eventuali disposizioni indicate dal soggetto designato o dal responsabile esterno, per il cui rispetto potranno essere effettuate verifiche ispettive interne da parte del titolare del trattamento e del responsabile della protezione dei dati personali;
- adottano ogni misura idonea a ridurre il rischio di distruzione o perdita dei dati o di accesso non autorizzato, segnalando al soggetto designato eventuali situazioni di rischio;
- rispettano gli obblighi di segretezza e di non divulgazione dei dati di cui vengono a conoscenza;
- trattano i dati di cui si viene a conoscenza in modo lecito, corretto e secondo il principio di necessità e di non eccedenza. L’incaricato ha accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;
- 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;
- 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;
- informano il titolare del trattamento e il Responsabile della protezione dei dati, senza ingiustificato ritardo, di ogni violazione dei dati personali di cui agli art. 33 e 34 del GDPR.

Art. 35 - Il Responsabile della Protezione dei Dati (RPD)

Il Responsabile della Protezione dei Dati, o Data Protection Officer, 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 GDPR.
L’Azienda pubblica i dati di contatto del RPD e li comunica all'Autorità Garante della Protezione dei dati personali in conformità alle indicazioni di tale Autorità, e si assicura che sia tempestivamente e adeguatamente coinvolto su tutte le questioni riguardanti la protezione dei dati personali.
Il Direttore Generale fornisce al Responsabile della Protezione dei Dati le risorse umane, tecnologiche, strumentali ed economiche necessarie per assolvere ai suoi compiti, accedere ai dati personali e ai trattamenti e mantenere la propria conoscenza specialistica.
Il RPD può avvalersi di referenti per la privacy individuati in modo capillare nell’ambito delle varie strutture dell’Azienda e si assicura della massima collaborazione del servizio USIS-CED, e di ogni altra articolazione aziendale che gestisce le infrastrutture e le Tecnologie di Informazione e Comunicazione, in merito all’applicazione interna delle misure di sicurezza e di protezione dei dati personali per i trattamenti automatizzati adottati.
Il RPD attiva tutte le misure per favorire l’osservanza del presente documento e delle altre disposizioni vigenti relative alla protezione dei dati e svolge altresì i seguenti compiti:

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

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

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

Art. 36 - Gli amministratori di sistema

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”.
Gli amministratori di sistema vengono nominati previa valutazione dell’esperienza, capacità e affidabilità dei soggetti designati, i quali devono 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.

Parte quarta – Misure tecniche ed organizzative

Art. 37 - Le misure di sicurezza

Il titolare del trattamento ed i responsabili del trattamento dei dati sono tenuti ad adottare, così come previsto dalle disposizioni vigenti in materia di protezione dei dati e di amministrazione digitale, ogni misura di sicurezza necessaria per assicurare un livello sufficiente di sicurezza dei dati personali trattati.
Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, l’Azienda mette in atto di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e/o la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

Nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
Tutti coloro che trattano dati per conto dell'Azienda possono trattare dati personali solo se autorizzati e istruiti in tal senso dall'Azienda stessa.
L'accesso ad ogni procedura informatica è consentito solo se congruente con il trattamento dei dati per il quale si è stati formalmente autorizzati ed è consentito soltanto utilizzando apposite credenziali di autorizzazione fornite dall'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.

Art. 38 - La tenuta in sicurezza di documenti ed archivi

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

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

Si rinvia per ulteriori dettagli a quanto previsto da specifici regolamenti aziendali.

Art. 39 - Misure organizzative per la tutela della riservatezza

Presso tutti i presidi dell'Azienda sono adottate soluzioni organizzative atte a garantire la riservatezza degli utenti quali:

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

Nell'ambito delle misure organizzative per la tutela della riservatezza, l'Azienda si assicura del rispetto di obblighi di riservatezza da parte del personale delle ditte aggiudicatarie dei seguenti servizi che prevedono l'intervento di personale esterno nei locali dell'Azienda con possibile accesso, anche occasionale o fortuito, a dati personali di cui essa è titolare:

- servizio di pulizia e sanificazione;
- servizio di supporto assistenziale e di ausiliariato;
- servizio trasporti pazienti barellati
- studenti e volontari non autorizzati al trattamento dei dati.

Art. 40 - Norme e regolamenti in materia di privacy e tutela della riservatezza

Il trattamento dei dati viene effettuato da personale soggetto al segreto professionale o al segreto d'ufficio. Si richiamano al riguardo, in modo non esaustivo, le principali disposizioni normative e regolamentari a tutela della privacy e della riservatezza:

- DPR n. 62/2013, "Regolamento recante codice di comportamento dei dipendenti pubblici", art. 12 - Rapporti con il pubblico - comma 5:
  "*Il dipendente osserva il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali e, qualora sia richiesto oralmente di fornire informazioni, atti, documenti non accessibili tutelati dal segreto d'ufficio o dalle disposizioni in materia di dati personali, informa il richiedente dei motivi che ostano all'accoglimento della richiesta. Qualora non sia competente a provvedere in merito alla richiesta cura, sulla base delle disposizioni interne, che la stessa venga inoltrata all'ufficio competente della medesima amministrazione*".
- Codice etico approvato con deliberazione n. 100 del 28 gennaio 2015 ed in particolare l'art. 7 con il quale viene fatto divieto a tutti i dipendenti, collaboratori e altri soggetti comunque presenti in Azienda, di effettuare qualunque tipo di ripresa video, fotografica e registrazioni audio di qualunque natura, non autorizzata e di pubblicare sulle proprie pagine di social network, e comunque su siti internet, dati personali, ad esempio nomi o fotografie, di pazienti e qualunque altro contenuto in contrasto con i principi e le regole del codice etico.
- Codice di comportamento aziendale aggiornato con deliberazione n. 384 del 4 marzo 2019, con particolare riferimento alle parti di seguito richiamate:
  Art. 3 - Principi generali, comma 3, lettera e):
  "*L'azienda garantisce nel trattamento delle informazioni il rispetto delle previsioni normative e regolamentari in materia di tutela e protezione dei dati personali, con particolare riguardo ai dati relativi alla salute e alla dignità della persona e del segreto d'ufficio. I dipendenti, fatte salve le norme a tutela della privacy, sono tenuti a fornire tutte le informazioni necessarie agli utenti e, nel farlo, devono usare un linguaggio chiaro, semplice e comprensibile, motivando le risposte e cooperando con riservatezza".*
  Art. 8 – Trasparenza e tracciabilità, comma 3
  "La tenuta e la conservazione della documentazione amministrativa e/o sanitaria deve avvenire nel rispetto della normativa privacy."
  Art. 10 - Comportamento in servizio, comma 2:
  "I destinatari del Codice […]:
  - rispettano il segreto d'ufficio e mantengono riservate le notizie e le informazioni apprese nell'ambito dell'attività svolta;

- non divulgano le informazioni relative ai procedimenti in corso, prima che siano stati ufficialmente deliberati dagli organi competenti, fermo restando i diritti degli interessati al procedimento; […]
- si astengono dal rendere pubblico con qualunque mezzo, compresi il web o i social network, i blog o i forum, commenti, informazioni e/o foto/video/audio che possano ledere l'immagine dell'Azienda, l'onorabilità dei colleghi, nonché la riservatezza o la dignità delle persone e in particolare dei pazienti;"
Art. 11 - Comportamento nei rapporti con il pubblico e con i mezzi di informazione, comma 8:
"Nei rapporti con gli organi di informazione, particolare attenzione deve essere posta alla tutela della riservatezza e della dignità delle persone e al diritto alla protezione dei dati personali e dei dati relativi alla salute."
Art. 15 - Ricerca e sperimentazioni, comma 3:
[…] "Lo svolgimento di tale attività avviene altresì nel rispetto dei seguenti requisiti:
- completa informativa al paziente in merito alla sperimentazione e/o studio e conseguente acquisizione del consenso informato, ove necessario;
- conformità ai principi della normativa in materia di protezione dei dati personali;"
Art. 18 - Attività conseguenti al decesso in ambito ospedaliero, comma 1, lettera a):
"i destinatari coinvolti […] rispettano l'obbligo di riservatezza relativo all'evento del decesso;"

Art. 41 - Sensibilizzazione e formazione

L'Azienda promuove al suo interno ogni iniziativa di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.
In tale ottica una delle iniziative di sensibilizzazione è costituita dall'attività formativa ed informativa rivolta al personale aziendale ed a tutti coloro che intrattengono rapporti con l'Azienda.
Oltre a specifiche attività formative finalizzate al continuo aggiornamento dei soggetti autorizzati al trattamento dei dati personali, l'Azienda, al fine di garantire la conoscenza capillare delle disposizioni contenute nel GDPR e nel presente Regolamento, allestisce all'interno del proprio portale internet e nel sito intranet aziendale apposite sezioni dedicate al tema della protezione dei dati personali contenenti le informative sul trattamento dei dati personali, la modulistica da usare nello svolgimento delle attività istituzionali ed ogni altra documentazione di riferimento e di supporto.
Inoltre, ad ogni dipendente di nuova assunzione viene consegnata una specifica comunicazione con i riferimenti per l'acquisizione e la consultazione del presente Regolamento. Il dipendente, acquisita tale comunicazione, si impegna a scaricare copia, prendere visione ed attenersi alle prescrizioni aziendali in materia di protezione dei dati personali.

Art. 42 - Il registro delle attività di trattamento

Il titolare del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità, contenente le informazioni di cui all'art. 30, paragrafo 1, del GDPR:

a) il nome e i dati di contatto del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati
g) 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 del titolare, contenente le informazioni di cui all'art. 30, paragrafo 2, del GDPR.

I Registri sono tenuti in forma scritta, anche in formato elettronico e, su richiesta, vengono messi a disposizione dell'Autorità Garante per la protezione dei dati personali.

Art. 43 - La valutazione di impatto sulla protezione dei dati e la consultazione preventiva

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un elevato rischio per i diritti e le libertà delle persone fisiche, l'Azienda, prima di procedere al trattamento dei dati personali, effettua una valutazione d'impatto ai sensi dell'articolo 35 del GDPR consultandosi con il Responsabile della Protezione dei Dati. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi analoghi.
Per le tipologie di trattamenti soggette al requisito di una valutazione d'impatto sulla protezione dei dati si rinvia all'elenco, non esaustivo, allegato alla delibera n. 467 del 11/10/2018 del Garante per la protezione dei dati personali (G.U. n. 269/2018).
La valutazione d'impatto 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; e
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Se necessario l'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 protezione dei dati personali secondo le modalità previste dall'art. 36 del GDPR.

Art. 44 - La violazione dei dati personali

Ogni responsabile o soggetto designato /incaricato del trattamento dei dati personali è tenuto ad informare senza ingiustificato ritardo l'Azienda del possibile caso di violazione dei dati personali (data breach) di cui agli art. 33 e 34 del GDPR.
Ogni interessato può inoltre 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 dei Responsabili del trattamento e dei soggetti designati/autorizzati, accerta l'effettivo stato dell'arte.
L'Azienda provvede a notificare la violazione all'Autorità Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli Interessati. Qualora la notifica non sia effettuata entro 72 ore, questa è corredata dei motivi del ritardo.
La notifica della violazione dei dati personali deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;

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

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
L'Azienda tiene aggiornato un registro con il quale documenta qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio; tale documentazione consente al Garante per la protezione dei dati personali 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.
Indipendentemente dalla necessità di segnalazione all'Autorità di controllo ed all'interessato, l'Azienda istituisce un registro di Data Breach in formato elettronico tenuto dal Responsabile per la protezione dei dati personali.

Parte quinta – Norme finali e sanzioni

Art. 45 - 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 aziendali in materia di trattamento dei dati personali.
I controlli e le verifiche sono effettuati periodicamente o, in caso di necessità, anche su sollecitazione degli interessati e le relative attività sono svolte dal personale a ciò incaricato sotto il coordinamento del DPO.

Art. 46 - Responsabilità in caso di violazione delle disposizioni sulla protezione dei dati

La violazione delle disposizioni richiamate all'articolo 166, comma 1 e 2, del D. Lgs. 196/2003 comporta l'applicazione delle sanzioni amministrative pecuniarie di cui all'art. 83, paragrafo 4 e 5, del GDPR. Con riferimento alle specifiche attività svolte dall'Azienda, si riporta di seguito un prospetto di sintesi con i riferimenti agli articoli del D. Lgs. 196/2003 oggetto di sanzione amministrativa, rinviando alla consultazione integrale delle norme qui richiamate:

Sanzione amministrativa art. 83, paragrafo 4, del GDPR (fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore)	
Violazione	Oggetto
Art. 2-quinquiesdecies	Prescrizioni del Garante nel caso di trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico
Art. 92, comma 1	Cartelle cliniche
Art. 93, comma 1	Certificato di assistenza al parto
Art. 110, comma 1	Valutazione di impatto in caso di ricerca medica, biomedica ed epidemiologica, consultazione preventiva del Garante

Sanzione amministrativa art. 83, paragrafo 5, del GDPR (fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore)	
Violazione	Oggetto
Art. 2-ter	Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri
Art. 2-sexies	Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante
Art. 2-septies, comma 7	Utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati
Art. 2-octies	Principi relativi al trattamento di dati relativi a condanne penali e reati
Art. 2-terdecies, commi 1, 2, 3 e 4	Diritti riguardanti le persone decedute
Art. 52, commi 4 e 5	Dati identificativi degli interessati contenuti nei provvedimenti dell'autorità giudiziaria
Art. 75	Trattamento di dati personali per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività
Art. 78	Informazioni del medico di medicina generale o del pediatra
Art. 79	Informazioni da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio-sanitarie
Art. 80	Informazioni da parte di altri soggetti
Art. 82	Emergenze e tutela della salute e dell'incolumità fisica
Art. 92, comma 2	Richieste di visione o rilascio di copia di cartelle cliniche da parte di soggetti diversi dall'interessato
Art. 93, commi 2 e 3	Certificato di assistenza al parto
Art. 96	Trattamento di dati relativi a studenti
Art. 99	Durata del trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici
Art. 100, commi 1, 2 e 4	Dati relativi ad attività di studio e ricerca
Art. 101	Trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica
Art. 105 commi 1, 2 e 4,	Trattamento a fini statistici o di ricerca scientifica
Art. 110-bis, commi 2 e 3	Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici
Art. 111	Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro
Art. 111-bis	Informazioni in caso di ricezione di curriculum
Art. 157	Richiesta di informazioni e di esibizione di documenti da parte del Garante
Art. 2-septies e 2-quater	Misure di garanzia e regole deontologiche

Il trattamento illecito di dati personali comporta l'applicazione delle misure di natura penale richiamate dagli art. da 167 a 172 del D. Lgs. n. 196/2003.

La violazione delle norme di comportamento in materia di trattamento dei dati personali costituisce violazione dei doveri d'ufficio e comporta l'applicazione di sanzioni disciplinari così come previsto dalla legge, dai regolamenti e dai contratti collettivi.

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

Art. 47 - Norma finale

Per quanto non espressamente previsto nel presente Regolamento, si fa rinvio al Regolamento (UE) 2016/679 del 27.04.2016, ed al Decreto Legislativo n. 196/2003, così come modificato con D. Lgs. n. 101/2018, nonché ai provvedimenti specifici del Garante per la protezione dei dati personali ed alle correlate disposizioni normative.

Il presente Regolamento entra in vigore ad intervenuta esecutività della relativa delibera di approvazione e sostituisce il Regolamento approvato con deliberazione n. 78 del 23 maggio 2018 ed ogni altra precedente regolamentazione interna nella medesima materia.

Il Regolamento viene pubblicato sul sito aziendale www.policlinicovittorioemanuele.it, pagina “Amministrazione Trasparente”, sezione “Atti generali”, sottosezione “Regolamenti aziendali” e nella pagina “Tutela della privacy”.