COPIA ATTI ARCHIVIO

ENTE OSPEDALIERO SPECIALIZZATO IN GASTROENTEROLOGIA
"Saverio de Bellis"
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Ente di Diritto Pubblico D.M. del 31.3.1982
Via Turi, 27
70013 CASTELLANA GROTTE (BARI)

DELIBERAZIONE DEL DIRETTORE GENERALE
Nominato con "D.P.G.R. n.61 del 07.02.2018"

DELIBERAZIONE N. 19 DEL 10 GEN. 2019

OGGETTO: Regolamento interno per la protezione dei dati delle persone fisiche. Determinazioni.

UFFICIO PROPONENTE: Affari Generali

il redigente del procedimento amm.vo
dott. Simone Montanaro

ATTESTAZIONE DI REGOLARITA' TECNICA:
Si attesta la conformità dell'atto alle normative nazionali e regionali in materia.

il dirigente dell'ufficio proponente
dott. Fabio Scattarella

ATTESTAZIONE DI REGOLARE IMP.NE DELLA SPESA :

il dirigente dell'U.o.c. economico-finanziaria
dott. Giuseppe Savino

Il Dott. Tommaso A. Stallone, Direttore Generale dell'Ente,

Premesso che:

- il Parlamento europeo ed il Consiglio in data 27 aprile 2016 hanno approvato il Regolamento UE 679/2016 (GDPR- *General Data Protection Regulation)* relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;
- il testo, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, è divenuto definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018, dopo un periodo di transizione di due anni, in quanto non richiede alcuna forma di legislazione applicativa o attuativa da parte degli stati membri;
- il Garante per la protezione dei dati personali ha emanato una Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali che intende offrire un panorama delle principali problematiche che i soggetti pubblici, oltre alle imprese, dovranno tenere presenti con la piena applicazione del Regolamento ;
- ai sensi dell'art.13 della Legge n.163/2017 il Governo è stato delegato ad adottare, entro sei mesi dalla sua entrata in vigore, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del 27 aprile 2016 di che trattasi;
- il decreto legislativo 10 agosto 2018, n. 101 è stato pubblicato in G.U. in data 4 settembre 2018 n.205, e reca disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

Considerato che :

- che risulta necessario avviare un percorso di profondo cambiamento, anche culturale, che consenta una protezione dei dati di tipo sostanziale, in luogo di un approccio meramente formale, nel pieno rispetto dei diritti e delle libertà fondamentali dei cittadini ;

- L'attuale assetto dei soggetti e delle responsabilità connesse al trattamento dei dati personali, è basato sulla disciplina in materia di protezione dei dati ;

- il Titolare può designare sotto la propria responsabilità e all'interno del proprio assetto organizzativo, le persone fisiche a cui attribuire compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati;

quanto previsto dall'art. 4 del RGPD (Regolamento Generale per la protezione dei dati) in ordine alla figura e ruolo di :

✓ Titolare del trattamento , quale persona fisica o giuridica che determina le finalità ed i mezzi del trattamento dei dati personali [c. 1, n.7];

✓ Responsabile del trattamento, quale persona fisica o giuridica che tratta i dati personali per conto del Titolare[c. 1, n.8];

✓ Terzo, quale persona fisica o giuridica autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare [c. 1, n.10];

Tenuto conto :

che quanto previsto dall'art. 29 del D.Lgs 196/03 in ordine al Responsabile interno del trattamento non trova più riscontro nel RGPD;

dell'indirizzo espresso dall' Autorità Garante per la protezione dei dati in ordine alla figura dell' "incaricato" al trattamento dei dati personali, introdotto dall'art. 30 del D.Lgs 196/03 che pur non espressamente prevista dal RGPD, è individuata nelle persone "autorizzate dal Titolare o Delegato al trattamento" ;

che la figura del Responsabile del trattamento definita dall'art. 4 c.1 par.8 del RGPD si riferisce a Soggetti esterni che trattano dati in esecuzione di un contratto o di altro atto giuridico che disciplina i processi, le procedure, gli strumenti e gli obblighi di qualità e di vigilanza (art. 8 c. 3 del RGPD) contratti con il Titolare ;

Preso atto :

che questo IRCCS, con deliberazione del Direttore Generale n. 552 del 25/10/2016, ha provveduto a nominare quali Responsabili interni del trattamento dei dati, ai sensi e per gli effetti dell'art. 29 del D.Lgs. n. 196/2003 (ora abrogato dal D.lgs. 101/2018), tutti i Direttori/Dirigenti Responsabili pro-tempore, apicali e delle UO Complesse, Semplici e Semplici Dipartimentali, stabilendo nel contempo che dovessero intendersi quali "incaricati", ai sensi e per gli effetti dell'art.30 del suddetto decreto legislativo, tutti gli altri dipendenti e collaboratori dell'IRCCS;

che il RGPD prevede che il Titolare del trattamento possa nominare quelli che vengono ora denominati "delegati per la protezione dei dati" e che lo stesso Titolare, o i delegati, possano individuare le "persone autorizzate al trattamento dei dati" così come previsto dall'art. 2-quaterdecies del decreto legislativo n. 101 del 10 agosto 2018, che ha modificato il Codice in materia di protezione dei dati personali;

Considerato :

che le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali e tecnici che il Titolare del trattamento dei dati personali deve, fin da subito, considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di protezione dei dati personali;
che appare necessario ed opportuno stabilire modalità organizzative, misure procedimentali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano a questo IRCCS di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento;

Visto :

lo schema di Regolamento interno relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, in allegato alla presente deliberazione per farne parte integrante e sostanziale;

Preso atto :

che ciascun Dirigente è designato dal Titolare del trattamento quale "Delegato per la protezione dei dati, in conformità al RGPD" con il compito di assicurare quanto necessario per un adeguato indirizzo ed organizzazione delle Strutture di competenza, ivi compreso il coordinamento delle attività del trattamento effettuate dai soggetti che a qualsiasi titolo vi operano in attuazione del RGPD;

in relazione al contesto organizzativo di questo IRCCS sono designati **"Delegati per la protezione dei dati"**, in conformità al Regolamento Generale sulla protezione dei dati (in sigla RGPD), **tutti i Direttori/Dirigenti Responsabili pro-tempore, apicali e delle U.O. Complesse, Semplici e Semplici Dipartimentali;**

- i "Delegati per la protezione dei dati", così individuati, devono provvedere a tutte le attività previste dal RGPD e a tutti i compiti loro affidati in ragione delle rispettive competenze, tenuto conto delle materie trattate, della durata, della natura e della finalità del trattamento o dei trattamenti assegnati, del tipo di dati personali oggetto di trattamento e delle categorie di interessati, degli obblighi e dei diritti del Titolare del trattamento, così come rinvenienti dagli atti deliberativi e dai modelli organizzativi in essi richiamati;

- in particolare, ciascun "Delegato per la protezione dei dati" è tenuto ad eseguire direttamente, nell'ambito delle istruzioni fornite dal Titolare del trattamento, quanto di seguito specificato :

  a) **autorizzare al trattamento dei dati personali ciascun dipendente mediante atto individuale che** :

- specifichi il ruolo operativo assegnato all'interno della propria unità operativa;

- contenga le specifiche istruzioni rapportate alla funzione operativa, alle procedure e strumenti autorizzati per ciascun incaricato e relativo profilo applicativo;

- vincoli i soggetti autorizzati al trattamento dei dati all'obbligo di riservatezza.

  Il modello di designazione dei dipendenti, in qualità di soggetti autorizzati al trattamento dei dati personali, è allegato al presente atto per farne parte integrante e sostanziale (ALLEGATO_1- Atto nomina soggetti autorizzati).

  b) porre in essere tutte le attività necessarie all'adeguamento dei trattamenti dei dati alle norme contenute nel RGPD, nonché alle norme nazionali e attuative;

  c) collaborare e partecipare alla predisposizione ed aggiornamento continuo del registro delle attività di trattamento, secondo le indicazioni operative che saranno fornite d'intesa con il RPD;

  d) **Mettere in atto, con il supporto dell'Unità Operativa "Controllo di Gestione e Sistemi Informativi", le misure tecniche ed organizzative a garantire un livello di sicurezza adeguato al rischio**, che comprendano, tra le altre, se del caso :

     ✓ La pseudonimizzazione e la cifratura dei dati personali;

     ✓ La capacità di assicurare su base permanente la riservatezza, integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento dei dati;

- ✓ La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

- ✓ Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.

e) provvedere alla sensibilizzazione e formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo, compatibilmente con le disponibilità di bilancio;

f) assistere il Titolare e il RPD nella conduzione della valutazione dell'impatto sulla protezione dei dati, ai sensi dell'art. 35 del RGPD;

g) informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (*cd. "data breach"*), per la successiva notifica della violazione all'Autorità Garante per la protezione dei dati, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati;

h) formalizzare, tramite gli Uffici preposti, il/i contratto/i da cui scaturiscono gli obblighi ex art. 28 paragrafo 3 del RGPD a carico dei Responsabili "esterni" del trattamento, ossia dei soggetti pubblici o privati affidatari di attività e servizi per conto di questo IRCCS, relativamente alle banche dati gestite da soggetti esterni in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

i) adottare, con riferimento ai rapporti in essere con i Responsabili "esterni", ogni iniziativa utile ad acquisire notizie relative all'adeguamento alle norme del RGPD, ponendo a loro carico ogni ulteriore onere informativo e/o dichiarativo nei confronti di questo IRCCS;

j) individuare eventuali conTitolari del trattamento, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, ai sensi dell'art. 26 del RGPD;

Utilizzare la nuova modulistica sulle informazioni da rendere agli Assistiti con riguardo al trattamento dei dati personali, ai sensi degli artt. 13-14 del RGPD. Le informazioni sono rese agli Assistiti dai Dirigenti/Responsabili di ciascuna Struttura/U.O./Servizio/Reparto, con modalità idonee quali l'inserimento del modulo delle informazioni sul trattamento dei dati in cartella clinica, l'affissione di appositi cartelli nelle sale d'attesa e negli altri locali di affluenza del pubblico; mediante la pubblicazione delle informazioni sul sito internet istituzionale; mediante stampa o invio tramite email su esplicita richiesta dell'interessato.

La modulistica aggiornata sulle informazioni da rendere agli Assistiti, ai sensi degli artt. 13-14 del RGPD, che si allega al presente atto per farne parte integrante e sostanziale, sarà pubblicata sul sito internet istituzionale, nell'apposita sezione Privacy e dovrà essere utilizzata dai Dirigenti/Responsabili in base alle finalità principali perseguite, come di seguito indicato:

allegato n.2 (ALLEGATO_2-INFORMATIVA-ASSISTITI-PRESTAZIONI-GDPR_2018) : da utilizzare nell'ambito delle prestazioni sanitarie offerte in regime di ricovero/ambulatoriale/ALPI e da stampare o inviare tramite email, su richiesta dell'Assistito o suo rappresentante legale;

allegato n.3 (ALLEGATO_3-POSTER-INFORMATIVA-ASSISTITI-PRESTAZIONI-GDPR_2018) : da utilizzare nell'ambito delle prestazioni sanitarie offerte in regime di ricovero/ambulatoriale/ALPI tramite affissione di cartelli nelle sale d'attesa e nei locali di affluenza del pubblico;

allegato n.4 (ALLEGATO_4-Modulo-INFORMATIVA-ASSISTITI-AMMINISTRATIVO_GDPR_2018) : da utilizzare nell'ambito delle attività amministrative correlate alle prestazioni sanitarie (CUP, URP etc.) e da stampare o inviare tramite email, su richiesta dell'Assistito o suo rappresentante legale;

allegato n.5 (ALLEGATO_5-POSTER-INFORMATIVA-ASSISTITI-AMMINISTRATIVO_GDPR_2018) : da utilizzare nell'ambito delle attività amministrative correlate alle prestazioni sanitarie (CUP, URP etc.) tramite affissione di cartelli nei locali di affluenza del pubblico;

allegato n.6 (ALLEGATO_6-Modulo-CONSENSO-ASSISTITI_GDPR_2018) : da utilizzare nell'ambito delle prestazioni sanitarie offerte in regime di ricovero e da far compilare e firmare all'Assistito o suo rappresentante legale e da custodire in cartella clinica.

k) adottare misure organizzative ed operative adeguate per il soddisfacimento delle richieste di esercizio dei diritti riconosciuti all'interessato ed espressamente disciplinati agli artt. 12 e seguenti del RGPD ;

l) collaborare con il Responsabile della protezione dei dati (RPD ai sensi del RGPD artt. 37 e 39) al fine dell'individuazione dei trattamenti eseguiti e della loro conformità al RGPD;

m) consentire al RPD ed eventuali Terzi incaricati, l'accesso agli uffici, banche dati e sistemi informatici durante gli *audit* interni periodici concordati con il Titolare del trattamento dei dati;

n) vigilare affinchè nessun soggetto privo di autorizzazione possa operare nelle strutture aziendali;

Con successiva nota sarà notificato a ciascun Dirigente l'atto individuale di delega al trattamento dei dati, comprendente le istruzioni specifiche del Titolare del trattamento.

Ritenuto

opportuno procedere all'approvazione dell'allegato "Regolamento interno per la protezione dei dati delle persone fisiche", per permettere a questo IRCCS di provvedere con immediatezza all'attuazione del Regolamento UE 2016/679;

D E L I B E R A

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

- di approvare il Regolamento in materia di protezione dati personali che viene allegato al presente atto per farne parte integrante e sostanziale;

- di stabilire che tutti i dirigenti, dipendenti e collaboratori, in qualità di Delegati per la protezione dei dati personali, in conformità al RGPD, sono tenuti nelle forme previste dal presente Regolamento, a fornire ampia collaborazione e supporto al Responsabile della protezione dei dati designato, nel complessivo processo di adeguamento dinamico alla protezione dei dati personali;

- di dare mandato all'Unità Operativa Controllo di Gestione e Sistemi Informativi di mettere in atto misure tecniche, informatiche e organizzative adeguate, ai sensi dell'art. 32 del RGPD, per garantire ed essere in grado di dimostrare che i trattamenti dei dati personali svolti presso questo IRCCS vengono effettuati in conformità alla vigente normativa nazionale ed europea;

- di dare atto che con successivi provvedimenti, adottati dai soggetti competenti di questo IRCCS, si procederà secondo la disciplina contenuta nel presente atto ed in conformità a quanto stabilito nel Regolamento UE 2016/679 e successivi decreti attuativi, ed in particolare:

- alla nomina dei Responsabili del trattamento (aziende esterne) con onere a carico degli Uffici preposti;

- all'istituzione dei registri delle attività di trattamento con il supporto dei Delegati per la protezione dei dati personali;

- a mettere in atto misure tecniche e organizzative adeguate, ai sensi dell'art. 32 del RGPD, per garantire ed essere in grado di dimostrare che i trattamenti dei dati personali vengono effettuati in conformità alla disciplina europea in materia di protezione dei dati personali;

- all'aggiornamento della documentazione in essere in relazione ai trattamenti dei dati personali (informativa e consenso ove necessario);

- di dichiarare il presente atto immediatamente eseguibile, attesa la necessità di assolvere con urgenza gli adempimenti consequenziali.

- di disporre che il presente atto venga pubblicato nell'albo pretorio online.

La presente deliberazione si compone di n.10 pagine e n. 8 allegati

Parere favorevole il **Direttore amministrativo**
Dott.ssa Filomena Fortunato

Parere favorevole il **Direttore sanitario**
Dott. Roberto Di Paola

Parere _____ il **Direttore scientifico**
(per quanto di competenza) Prof. Gianluigi Giannelli

il **DIRETTORE GENERALE**
Dott. Tommaso A. Stallone

Castellana Grotte, il 18 GEN. 2019

ATTESTATO DI PUBBLICAZIONE

Si attesta che copia della deliberazione viene pubblicata sull'Albo on line sul sito WEB di questo Ente a partire dal 22 GEN. 2019.

l'incaricato alla pubblicazione

il Funzionario amm.vo AA.GG.

ALL. N. 1 ALLA DDG
N° 19 DEL 10 GEN. 2019

Allegato 1. Atto nomina soggetti autorizzati

OGGETTO : ATTO DI NOMINA DELLE PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI

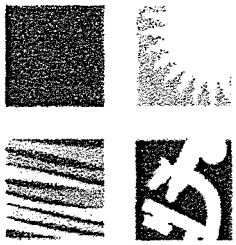
STRUTTURA/UNITA' : .....

DIRIGENTE/DIRETTORE:
.....

Il sottoscritto (Nome e Cognome_____)

Direttore/Dirigente (indicare struttura)..... ....., in qualità di "Delegato interno per la protezione dei dati" in conformità al Regolamento generale sulla protezione dei dati personali, giusta deliberazione del Direttore Generale ....., con il presente atto nomina la S.V. quale Soggetto autorizzato al trattamento dei dati presso (indicare Sede/Struttura/ UO)..... nella modalità cartacea ed informatica, nell'ambito dell'attività che effettivamente svolge per conto di questo IRCCS nel ruolo di .....
(sanitario, amministrativo, dottorando, borsista etc..)

In osservanza del Regolamento (UE) 2016/679 , che regola il trattamento dei dati personali, laddove costituisce trattamento *"qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati"*, ed in relazione al presente atto di nomina, **Lei è autorizzato al trattamento dei dati personali** *(tutti quei dati idonei a identificare direttamente o indirettamente una persona fisica)* **e dei dati appartenenti a**



categorie particolari *(dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona)* **la cui conoscenza ed il cui trattamento siano strettamente necessari per adempiere ai compiti assegnati.**

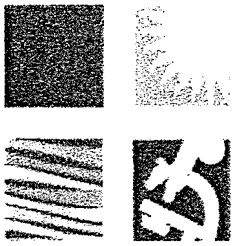
Nel trattamento dei dati **Lei** deve scrupolosamente attenersi alle seguenti istruzioni:

- trattare i dati in modo **lecito** e secondo **correttezza**;
- raccogliere i dati e registrarli per gli scopi inerenti l'attività svolta;
- verificare, ove possibile, che i dati siano esatti e, se necessario, aggiornarli;
- verificare che i dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Direttore/Dirigente della Struttura di appartenenza;
- mantenere la **massima riservatezza** sui dati di cui si effettua il trattamento;

non utilizzare, comunicare o diffondere alcuno dei dati predetti se non previamente autorizzato dal Titolare del trattamento o dal Direttore/Dirigente della Struttura di appartenenza;

- adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato;
- non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- in particolare, per quanto concerne l'utilizzo degli strumenti informatici, dovranno essere scrupolosamente osservate le disposizioni contenute nel vigente **"Regolamento per l'utilizzo e la gestione delle risorse strumentali informatiche e telematiche aziendali"**;
- per quanto concerne gli archivi cartacei, l'accesso è consentito solo se previamente autorizzato dal Titolare del trattamento o dal Direttore/Dirigente della Struttura di appartenenza e deve riguardare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere i compiti assegnati, avendo particolare riguardo a:

  - i documenti cartacei devono essere prelevati dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni;
  - atti e documenti contenenti dati sensibili o giudiziari devono essere custoditi in contenitori muniti di serratura e devono essere controllati in modo tale che a tali atti e documenti non possano accedere persone prive di autorizzazione;
  - atti e documenti contenenti eventuali dati sensibili o giudiziari devono essere restituiti al termine delle operazioni affidate;



- ☐ eventuali fotocopie di documenti devono essere autorizzate e custodite con le stesse modalità dei documenti originali;

E' vietata alla persona autorizzata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia funzionale allo svolgimento dei compiti affidati.
Per il trattamento dei dati devono essere seguite le norme di legge in materia di tutela della riservatezza dei dati personali e devono essere applicate le misure di protezione previste dal Titolare.
Ferma restando l'applicazione delle disposizioni vigenti in materia di trattamento dei dati sensibili e giudiziari e delle istruzioni impartite dal Titolare e dal Delegato per la protezione dei dati, i documenti ed i supporti recanti dati sensibili o giudiziari devono essere conservati in elementi di arredo muniti di serratura e non devono essere lasciati incustoditi in assenza della persona autorizzata.

Ciò premesso, nell'ambito della Sua qualifica di ..... Le viene conferito l'incarico di compiere le operazioni di trattamento sotto elencate, con l'avvertimento che dovrà operare osservando le direttive del Titolare/Delegato per la protezione dei dati e nel rispetto dei principi di cui in premessa.

Pertanto la S.V. è autorizzata a trattare

☐ **Tutte le banche dati di tipo PERSONALE, IVI COMPRESI I DATI APPARTENENTI A CATEGORIE PARTICOLARI (SENSIBILI E GIUDIZIARI), indispensabili per assolvere ai compiti assegnati**

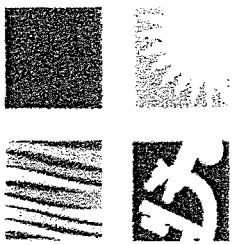
Ovvero

☐ **potrà avere accesso e trattare SOLO LE SEGUENTI BANCHE DATI**

BANCA DATI	Tipo permesso (lettura,modifica,inserimento,cancellazione,stampa, cancellazione)

Istruzioni specifiche da impartire al soggetto autorizzato:

Luogo e Data, ...



(firma del Direttore/Dirigente)

NOMINA DELLE PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI

Fac-simile REGISTRO FIRME PER PRESA VISIONE

STRUTTURA/UNITA' : .....

DIRIGENTE/DIRETTORE:
.....

Elenco nominativo delle persone autorizzate al trattamento dei dati

Nome e Cognome	Data	Firma (per presa visione)

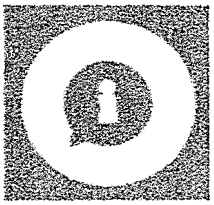
ALL. N. 2 ALLA DELIB
N° 19 DEL 18 GEN. 2019

ALLEGATO_2-INFORMATIVA-ASSISTITI-PRESTAZIONI-GDPR_2018

INFORMAZIONI PER GLI ASSISTITI

SUL TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DELLE PRESTAZIONI SANITARIE IN REGIME DI RICOVERO E AMBULATORIALE

Informazioni rese agli interessati secondo le disposizioni del Codice in materia di protezione dei dati personali (D.lgs. n. 196/2003 così come modificato dal D.lgs. n. 101/2018) ed in osservanza del Regolamento Generale sulla Protezione dei dati (UE) 2016/679

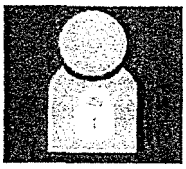


Gentile Utente,

Il Codice in materia di **protezione dei dati personali** (D.lgs. n. 196/2003 così come modificato dal D.lgs. n. 101/2018), in osservanza del Regolamento Generale sulla Protezione dei dati (Regolamento UE 2016/679), riconosce e disciplina il diritto alla protezione dei dati personali, **nel rispetto dei Suoi diritti e libertà fondamentali e della Sua dignità personale. Nella presente informativa sono riportate le informazioni relative al trattamento dei Suoi dati personali ed idonei a rivelare lo stato di salute, effettuati dall' I.R.C.C.S. "Saverio De Bellis"** (d'ora in avanti anche IRCCS) **per l'erogazione di prestazioni sanitarie.**

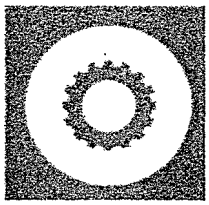
Il Titolare del trattamento è l' Azienda Ospedaliera specializzata in Gastroenterologia I.R.C.C.S. "Saverio De Bellis" con sede in Via Turi, 27 - 70013 a Castellana Grotte (Bari) , in persona del Direttore Generale pro-tempore, contattabile ai seguenti riferimenti :

Telefono: 080 4994167
email: direttoregenerale@irccsdebellis.it
pec : dirgenerale.debellis@pec.rupar.puglia.it



Il Responsabile della protezione dei dati personali è il Dott. Simone Montanaro, contattabile ai seguenti riferimenti :

Telefono 0804994162 email : simone.montanaro@irccsdebellis.it



FINALITÀ DEL TRATTAMENTO

L'Ente Ospedaliero Specializzato in Gastroenterologia "Saverio de Bellis" (d'ora in avanti IRCCS) è una struttura ospedaliera ad indirizzo specialistico gastroenterologico medico e chirurgico che opera in tale campo quale Istituto di Ricovero e Cura a Carattere Scientifico di diritto pubblico.
Le informazioni che La riguardano e che vengono raccolte in occasione di una visita, di un ricovero, di una terapia, di un esame o di un'altra prestazione sanitaria fornita dall'IRCCS, sono utilizzate per:

- tutela della salute, ossia **attività di diagnosi, assistenza e terapia sanitaria;**
- attività **amministrativo, gestionali e contabili,** correlate alle prestazioni sanitarie erogate anche tramite Convenzioni con altre strutture sanitarie autorizzate;

- attività di **programmazione, gestione, controllo e valutazione dell'assistenza sanitaria**, eventualmente svolte, previa Sua esplicita disponibilità, anche attraverso indagini e questionari di valutazione del gradimento;
- **attività certificatorie** relative allo stato di salute;
- **attività di ricerca medica, biomedica ed epidemiologica;**
- **attività di didattica** e formativa;
- ulteriori motivi di *c.d.* **interesse pubblico rilevante** previsti da norma di legge o di regolamento;
- altri adempimenti previsti da norme di legge o di regolamento.

Ulteriori trattamenti dei Suoi dati personali, che potrebbero presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, saranno effettuati, in conformità alle leggi e ai regolamenti, previa ulteriore nota informativa e previo suo specifico consenso. Si tratta ad esempio di trattamenti effettuati:

- ai fini di implementazione del Dossier Sanitario Elettronico o del Fascicolo Sanitario Elettronico;
- ai fini di implementazione dei sistemi di sorveglianza e dei registri di patologia;
- per scopi di ricerca scientifica nell'ambito delle sperimentazioni cliniche;
- nell'ambito della teleassistenza o telemedicina, al fine di consentire la trasmissione a distanza di tracciati e immagini, anche tramite un collegamento telematico bidirezionale con altre strutture autorizzate;
- ai fini dell'erogazione dei servizi di refertazione on-line;
- ai fini della crio-conservazione presso la Biobanca;
- ai fini della partecipazione a studi osservazionali;
- per attività di medicina *c.d.* predittiva.

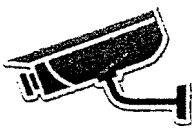
I dati trattati sono anagrafici (cognome, nome, sesso, data di nascita, luogo di nascita, provincia di nascita, indirizzo e luogo di residenza, provincia di residenza), identificativi (codice fiscale, SPID, CNS, TS-CNS e CIE) e relativi alla salute. Sono acquisiti anche i dati personali dei familiari o di terzi, ove necessario.

MODALITÀ DEL TRATTAMENTO DEI DATI PERSONALI

Per l'erogazione di una prestazione sanitaria, sia in regime ambulatoriale che di ricovero, Le verranno chiesti da parte degli operatori autorizzati dell'IRCCS i dati personali (nome, cognome, codice fiscale, tipo di esenzione, etc.) necessari ed obbligatori per provvedere ad erogarLe e/o prenotarLe la prestazione richiesta (ad esempio prenotazione della visita, ecc.). In caso di prenotazione di visita attraverso il sistema CUP o in altra occasione di contatto con l' IRCCS, oltre ai sopra citati dati personali, Le potrà essere richiesto anche un numero di telefono personale, fisso o cellulare ed un indirizzo e-mail che potranno essere utilizzati, fino a Sua diversa indicazione, per confermarLe o ricordarLe il giorno della prenotazione o per avvisarLa, anche tramite SMS, in caso di annullamento della visita o per finalità di prevenzione e di tutela di sanità collettiva e igiene pubblica.
E' altresì attivo sul sito internet istituzionale https://www.sanita.puglia.it/web/debellis/servizi-online il servizio di visualizzazione/disdetta online delle prenotazioni che prevede anche la procedura di pagamento del ticket online.
In caso di ricovero ospedaliero, i Suoi dati anagrafici ed i dati relativi al reparto in cui Lei è ricoverato/a saranno trattati per agevolare l'accesso ai reparti di degenza da parte dei visitatori; nel caso in cui Lei non intenda renderli disponibili, può manifestare l'eventuale specifico dissenso all'atto del ricovero. I dati da Lei rilasciati all' IRCCS verranno trattati esclusivamente dal personale debitamente autorizzato e istruito dall'IRCCS, e saranno conservati in luogo idoneo ed appropriato, tutelandone la riservatezza, nel rispetto del segreto professionale e d'ufficio. I suoi dati potranno inoltre essere trattati da società esterne, previamente nominate quali "Responsabili del trattamento dei dati" ai sensi dell'art. 28 del Regolamento, alle quali è affidato il compito di svolgere specifiche operazioni necessarie per garantire i servizi dell' IRCCS, nei limiti strettamente pertinenti alle finalità di cui sopra.

In merito alle attività didattiche, La informiamo che il perseguimento della formazione in ambito sanitario comporta, in occasione di alcune prestazioni sanitarie, la presenza di studenti autorizzati (c.d. medici in formazione specialistica, borsisti ecc.). L'IRCCS, al fine di limitare i disagi del paziente e in relazione al grado d'invasività del trattamento,

circoscrive il numero degli studenti presenti e garantisce il rispetto di eventuali legittime volontà contrarie del paziente.



VIDEOSORVEGLIANZA

In alcuni locali dell' IRCCS e lungo alcune aree perimetrali è attivo un sistema di videosorveglianza per ragioni di tutela della salute e sicurezza degli assistiti, dei visitatori e del personale nonché del patrimonio aziendale, adeguatamente segnalato da appositi cartelli informativi e gestito nel pieno rispetto di quanto stabilito nel Provvedimento in materia di videosorveglianza dell'8 aprile 2010 dell'Autorità Garante per la protezione dei dati personali ed in osservanza del Regolamento UE 2016/679. Per richiedere l'accesso alle sue immagini potrà inviare una richiesta direttamente al Titolare del trattamento oppure al Responsabile della protezione dei dati personali, ai contatti sopra indicati.

CONFERIMENTO E FONTE DEI DATI

Ad eccezione di eventuali obblighi di legge, il conferimento dei dati personali richiesti da parte dell' IRCCS è facoltativo, ma necessario al pieno raggiungimento delle finalità sopra indicate. Fatto salvo il superiore diritto alla salute dell'individuo, l'eventuale rifiuto di conferire in tutto o in parte i dati richiesti o la successiva richiesta di cancellarli potrebbe comportare per l'IRCCS l'impossibilità di eseguire o continuare, in tutto o in parte, l'attività richiesta o comunque inerente e/o conseguente allo svolgimento delle proprie funzioni istituzionali. I dati personali indispensabili per l'erogazione delle prestazioni richieste sono forniti direttamente dall'interessato o tramite terzi legittimati (ad es. l'anagrafe unica degli assistiti della Regione Puglia).

AMBITO DI COMUNICAZIONE

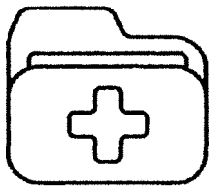
I dati personali e sensibili non possono essere diffusi ma possono essere comunicati, per le finalità segnalate, a soggetti terzi, se destinatari per norma o regolamento.
Tali dati potranno essere comunicati agli enti competenti per finalità istituzionali e/o amministrative, secondo quanto previsto dalla normativa vigente: in particolare, potranno essere comunicati, solo se necessario, ai seguenti soggetti:

- ai professionisti coinvolti nella gestione clinico-assistenziale;
- agli operatori amministrativi dell'IRCCS;
- ad altre Aziende Sanitarie e Associazioni in convenzione e alla Regione di appartenenza dell'utente;
- alla Compagnia Assicurativa dell'IRCCS per la tutela della stessa e dei suoi operatori, per le ipotesi di responsabilità;
- ad altri Soggetti pubblici (ad esempio Regione, Comune, INAIL...) o privati (a cui siano affidati compiti da parte dell'IRCCS) per finalità istituzionali di rilevante interesse pubblico;
- all'Autorità Giudiziaria e/o di Pubblica Sicurezza, nei casi espressamente previsti dalla legge.

Il trattamento dei dati può prevedere, in casi particolari, un processo di profilazione degli interessati in riferimento alle finalità del trattamento sopra indicate.
I dati personali potranno essere oggetto di trasferimento in paesi non appartenenti all'Unione Europea, unicamente relativamente a quelli in cui il livello di protezione è ritenuto adeguato dalla Commissione Europea ai sensi dell'art. 45 del Regolamento UE 2016/679. In qualsiasi momento potrà richiedere dettagli sui Paesi terzi, rivolgendosi al Titolare del trattamento o al Responsabile della protezione dei dati.

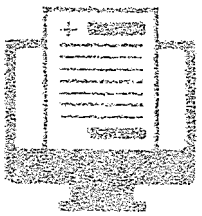
TEMPO DI CONSERVAZIONE

I dati personali ed idonei a rivelare lo stato di salute da Lei forniti e/o prodotti dall' IRCCS sono conservati nel rispetto delle vigenti normative in materia. In particolare, i dati relativi a ciascun episodio di ricovero, raccolti nella relativa cartella clinica (cartacea o elettronica), saranno conservati a tempo indeterminato. Le restanti tipologie di trattamento dati che l' IRCCS può effettuare e il periodo di conservazione di ciascuna tipologia di dati sono indicati dal Piano di conservazione dell'IRCCS.



DOSSIER SANITARIO ELETTRONICO

I Suoi dati personali potranno essere trattati, previo suo consenso, tramite un *Dossier* Sanitario Elettronico (DSE) ossia uno strumento informatizzato di raccolta di dati sanitari in formato elettronico, contenente diverse informazioni inerenti il Suo stato di salute o di colui che rappresenta legalmente, relative a eventi clinici presenti e pregressi, raccolte dall'IRCCS.
Il trattamento dei dati sanitari tramite il *Dossier* è effettuato al fine di migliorare i processi di diagnosi, assistenza e terapia sanitaria e permette ai professionisti sanitari dell'IRCCS di consultare le informazioni prodotte nell'ambito dell'intera Struttura sanitaria, e non solo quelle prodotte all'interno della singola unità operativa. Il consenso al trattamento dei dati sanitari attraverso il DSE viene manifestato all'IRCCS, attraverso la sottoscrizione con procedura manuale o informatica. E' possibile richiedere l'oscuramento di specifici eventi ed il consenso al DSE, una volta manifestato, potrà essere modificato o revocato in qualsiasi momento, rivolgendosi al Responsabile dell'Unità Operativa a cui ha richiesto la prestazione. Per maggiori informazioni sul Dossier sanitario si rinvia all'informativa estesa pubblicata sul sito internet istituzionale nella sezione dedicata "Privacy".



FASCICOLO SANITARIO ELETTRONICO

Il Fascicolo Sanitario Elettronico (FSE) è l'insieme di dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, che riguardano Lei o colui che rappresenta legalmente, prodotti dalle diverse Strutture Sanitarie e Socio-Sanitarie, volto a documentare la storia clinica sanitaria dell'Assistito.
Il FSE dei cittadini pugliesi è accessibile attraverso il link https://www.sanita.puglia.it/web/pugliasalute/fse, reso disponibile all'interno del Portale Regionale della Salute, la piattaforma unica di accesso ai servizi sanitari *on-line* della Regione Puglia.
Il FSE consente pertanto, previo suo consenso, di fornire un quadro clinico completo e particolareggiato, per offrirLe una migliore assistenza e cura quando si rivolge al Medico di Medicina Generale o al Pediatra di Libera Scelta oppure quando si reca presso una Struttura sanitaria o sociosanitaria del Servizio Sanitario Regionale. Per maggiori informazioni si rinvia all'indirizzo https://www.sanita.puglia.it/infofse.

I SUOI DIRITTI

In ogni momento potrà esercitare i Suoi diritti, secondo le modalità e le condizioni ivi indicate, previsti dagli articoli 15 e ss. del Regolamento (UE) 2016/679, tra cui quelli di chiedere all'IRCCS di :

- ottenere la conferma dell'esistenza o meno di dati personali che La riguardano, anche se non ancora registrati e la loro comunicazione in forma intellegibile;
- conoscere l'indicazione dell'origine dei dati personali, delle finalità e delle modalità di trattamento, nonché gli estremi identificativi dei responsabili del trattamento dei dati personali;
- conoscere l'indicazione degli estremi identificativi dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili del trattamento o persone designate e autorizzate al trattamento;
- ottenere l'aggiornamento, la rettifica ovvero l'integrazione dei dati che La riguardano;
- ottenere la cancellazione e la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
- opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta.

Lei ha altresì il diritto di :

- avanzare istanza volta a conoscere gli accessi eseguiti sui suoi dati personali all'interno del dossier sanitario;
- presentare reclamo all'Autorità Garante per la Protezione dei dati personali, in caso di illecito trattamento dei Suoi dati personali da parte dell'IRCCS, seguendo le procedure e le indicazioni pubblicate sul sito web dell'Autorità Garante www.garanteprivacy.it

I diritti di cui sopra sono esercitabili rivolgendosi direttamente al Titolare del trattamento dei dati o al Responsabile della protezione dei dati, ai contatti sopra riportati.

La versione sempre aggiornata di questa informativa è sempre rinvenibile sul sito web istituzionale all'indirizzo https://www.sanita.puglia.it/web/debellis.

INFORMAZIONI PER GLI ASSISTITI

SUL TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DELLE PRESTAZIONI SANITARIE IN REGIME DI RICOVERO E AMBULATORIALE

1. *Perché queste informazioni ?*

Gentile Utente,

Il Codice in materia di protezione dei dati personali (D.lgs. n. 196/2003 così come modificato dal D.lgs. n. 101/2018), in osservanza del Regolamento Generale sulla Protezione dei dati (Regolamento UE 2016/679), riconosce e disciplina il diritto alla protezione dei dati personali, nel rispetto dei Suoi diritti e libertà fondamentali e della Sua dignità personale. Nella presente informativa sono riportate le informazioni relative al trattamento dei Suoi dati personali ed idonei a rivelare lo stato di salute, effettuati dall'Ente Ospedaliero Specializzato in Gastroenterologia "Saverio de Bellis" (d'ora in avanti IRCCS) per l'erogazione di prestazioni sanitarie.

2. *Chi decide dei mie dati personali ?*

Il Titolare del trattamento dei dati è l'Azienda Ospedaliera specializzata in Gastroenterologia I.R.C.C.S. "Saverio De Bellis" con sede in Via Turi, 27 - 70013 a Castellana Grotte (Bari), in persona del Direttore Generale pro-tempore, contattabile ai seguenti riferimenti :

Telefono: 0804994167
email: direttoregenerale@irccsdebellis.it
pec : dirgenerale.debellis@pec.rupar.puglia.it

3. *Chi vigila sulla protezione dei miei dati ?*

Il Responsabile della protezione dei dati è il Dott. Simone Montanaro, contattabile ai seguenti riferimenti :

Telefono 0804994162 email : simone.montanaro@irccsdebellis.it

4. *Perché sono richiesti i miei dati ?*

FINALITÀ DEL TRATTAMENTO

L'Ente Ospedaliero Specializzato in Gastroenterologia "Saverio de Bellis" (d'ora in avanti IRCCS) è una struttura ospedaliera ad indirizzo specialistico gastroenterologico medico e chirurgico che opera in tale campo quale Istituto di Ricovero e Cura a Carattere Scientifico di diritto pubblico.
Le informazioni che La riguardano e che vengono raccolte in occasione di una visita, di un ricovero, di una terapia, di un esame o di un'altra prestazione sanitaria fornita dall'IRCCS, sono utilizzate per:

- tutela della salute, ossia attività di diagnosi, assistenza e terapia sanitaria;
- attività amministrativo, gestionali e contabili, correlate alle prestazioni sanitarie erogate anche tramite Convenzioni con altre strutture sanitarie autorizzate;
- attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, eventualmente svolte, previa Sua esplicita disponibilità, anche attraverso indagini e questionari di valutazione del gradimento;
- attività certificatorie relative allo stato di salute;
- attività di ricerca medica, biomedica ed epidemiologica;
- attività didattica e di formazione professionale previa anonimizzazione dei dati dell'assistito;
- ai fini di implementazione dei sistemi di sorveglianza e dei registri di patologia.

Ulteriori trattamenti dei Suoi dati personali, che potrebbero presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, saranno effettuati, in conformità alle leggi e ai regolamenti, previa ulteriore nota informativa e previo suo specifico consenso. Si tratta ad esempio di trattamenti effettuati ai fini di implementazione del Dossier Sanitario Elettronico o del Fascicolo Sanitario Elettronico. I dati trattati per l'esecuzione di compiti di interesse pubblico rilevante sono anagrafici (cognome, nome, sesso, data di nascita, luogo di nascita, provincia di nascita, indirizzo e luogo di residenza, provincia di residenza), identificativi (codice fiscale, SPID, CNS, TS-CNS e CIE) e relativi alla salute.

5. *Ci sono telecamere che mi riprendono ?*

VIDEOSORVEGLIANZA

In alcuni locali dell' IRCCS e lungo alcune aree perimetrali è attivo un sistema di videosorveglianza per ragioni di tutela della salute e sicurezza degli assistiti, dei visitatori e del personale nonché del patrimonio aziendale, adeguatamente segnalato da appositi cartelli informativi e gestito nel pieno rispetto di quanto stabilito nel Provvedimento in materia di videosorveglianza dell'8 aprile 2010 dell'Autorità Garante per la protezione dei dati personali ed in osservanza del Regolamento UE 2016/679. Per richiedere l'accesso alle sue immagini potrà inviare una richiesta al Titolare del trattamento dei dati oppure al Responsabile della protezione dei dati personali, ai contatti sopra indicati.

6. *Sono obbligato a fornire i dati ?*

CONFERIMENTO E FONTE DEI DATI

Il conferimento dei dati personali richiesti da parte dell' IRCCS è necessario al pieno raggiungimento delle finalità sopra indicate. Fatto salvo il superiore diritto alla salute dell'individuo, l'eventuale rifiuto di conferire in tutto o in parte i dati richiesti potrebbe comportare per l'IRCCS l'impossibilità di eseguire o continuare, in tutto o in parte, l'attività richiesta di diagnosi, assistenza e terapia sanitaria . I dati personali indispensabili per l'erogazione delle prestazioni richieste sono forniti direttamente dall'interessato o tramite terzi legittimati (ad es. l'anagrafe unica degli assistiti della Regione Puglia).

7. *Chi potrà conoscere i miei dati ?*

AMBITO DI COMUNICAZIONE

I dati personali e sensibili non possono essere diffusi ma possono essere comunicati, per le finalità segnalate, a soggetti terzi, se destinatari per norma o regolamento.
Tali dati potranno essere comunicati agli enti competenti per finalità istituzionali e/o amministrative, secondo quanto previsto dalla normativa vigente: in particolare, potranno essere comunicati, solo se necessario, ai seguenti soggetti:
ai professionisti coinvolti nella gestione clinico-assistenziale; agli operatori amministrativi dell'IRCCS;
ad altre Aziende Sanitarie e Associazioni in convenzione e alla Regione di appartenenza dell'utente;
alla Compagnia Assicurativa dell'IRCCS per la tutela della stessa e dei suoi operatori, per le ipotesi di responsabilità; ad altri Soggetti pubblici (ad esempio Regione, Comune, INAIL...) o privati (a cui siano affidati compiti da parte dell'IRCCS) per finalità istituzionali di rilevante interesse pubblico;
all'Autorità Giudiziaria e/o di Pubblica Sicurezza, nei casi espressamente previsti dalla legge.
Il trattamento dei dati può prevedere, in casi particolari, un processo di profilazione degli interessati in riferimento alle finalità del trattamento sopra indicate.

I dati personali potranno essere oggetto di trasferimento in paesi non appartenenti all'Unione Europea, unicamente relativamente a quelli in cui il livello di protezione è ritenuto adeguato dalla Commissione Europea ai sensi dell'art. 45 del Regolamento UE 2016/679. In qualsiasi momento potrà richiedere dettagli sui Paesi terzi, rivolgendosi al Titolare del trattamento o al Responsabile della protezione dei dati.

8. *Per quanto tempo sono conservati i miei dati ?*

TEMPO DI CONSERVAZIONE

I dati personali ed idonei a rivelare lo stato di salute da Lei forniti e/o prodotti dall' IRCCS sono conservati nel rispetto delle vigenti normative in materia. In particolare, i dati relativi a ciascun episodio di ricovero, raccolti nella relativa cartella clinica (cartacea o elettronica), saranno conservati a tempo indeterminato. Le restanti tipologie di trattamento dati che l' IRCCS può effettuare e il periodo di conservazione di ciascuna tipologia di dati sono indicati dal Piano di conservazione dell'IRCCS.

9. *Cosa è il Dossier Sanitario elettronico ?*

DOSSIER SANITARIO ELETTRONICO

I Suoi dati personali potranno essere trattati, previo suo consenso, tramite un Dossier Sanitario Elettronico (DSE) ossia uno strumento informatizzato di raccolta di dati sanitari in formato elettronico, contenente diverse informazioni inerenti il Suo stato di salute o di colui che rappresenta legalmente, relative ad eventi clinici presenti e pregressi, raccolte dall'IRCCS. Le informazioni di dettaglio sul trattamento dei dati tramite Dossier Sanitario sono disponibili sul sito internet istituzionale nell'apposita sezione "Privacy".

10. *Cosa è il Fascicolo Sanitario elettronico ?*

FASCICOLO SANITARIO ELETTRONICO

Il Fascicolo Sanitario Elettronico (FSE) è l'insieme di dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, che riguardano Lei o colui che rappresenta legalmente. Il FSE dei cittadini pugliesi è accessibile attraverso il Portale Regionale della Salute, la piattaforma unica di accesso ai servizi sanitari on line della Regione Puglia. Per maggiori informazioni si rinvia all'indirizzo web https://www.sanita.puglia.it/infofse.

11. *Quali sono i miei diritti ?*

I DIRITTI DELL'ASSISTITO

In ogni momento Lei potrà esercitare i diritti previsti dagli articoli 15 e ss. del Regolamento (UE) 2016/679, tra cui quelli di chiedere all'IRCCS di :

- **ottenere la conferma dell'esistenza** o meno di dati personali che La riguardano;
- **ottenere l'aggiornamento, la rettifica ovvero l'integrazione** dei dati che La riguardano;
- ottenere la **limitazione** dei dati trattati;
- **opporsi**, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta;
- presentare **reclamo** all'Autorità Garante per la Protezione dei dati personali, in caso di illecito trattamento dei Suoi dati personali da parte dell'IRCCS, seguendo le procedure e le indicazioni pubblicate sul sito web dell'Autorità Garante (www.garanteprivacy.it).

A chi posso rivolgermi ?

I diritti di cui sopra sono esercitabili rivolgendosi direttamente al Titolare del trattamento dei dati o al Responsabile della protezione dei dati, ai contatti sopra riportati (p.ti 2 e 3).
I modelli per l'esercizio dei diritti nonché le politiche aziendali in materia di protezione dei dati personali sono reperibili sul sito web aziendale all'indirizzo https://www.sanita.puglia.it/web/debellis nell'apposita sezione "Privacy".

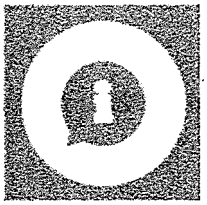
ALL. N. 4 ALLA DDS
N° 19 DEL 18 GEN. 2019

ALLEGATO_4-Modulo-INFORMATIVA-ASSISTITI-AMMINISTRATIVO_GDPR_2018

INFORMAZIONI PER GLI ASSISTITI

SUL TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DELLE ATTIVITA' AMMINISTRATIVE CORRELATE ALLE PRESTAZIONI SANITARIE

Informazioni rese agli interessati secondo le disposizioni del Codice in materia di protezione dei dati personali (D.lgs. n. 196/2003 così come modificato dal D.lgs. n. 101/2018) ed in osservanza del Regolamento Generale sulla Protezione dei dati (UE) 2016/679

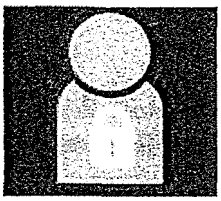


Gentile Utente,

Il Codice in materia di **protezione dei dati personali** (D.lgs. n. 196/2003 così come modificato dal D.lgs. n. 101/2018), in osservanza del Regolamento Generale sulla Protezione dei dati (Regolamento UE 2016/679), riconosce e disciplina il diritto alla protezione dei dati personali, **nel rispetto dei Suoi diritti e libertà fondamentali e della Sua dignità personale. Nella presente informativa sono riportate le informazioni relative al trattamento dei suoi dati personali ed idonei a rivelare lo stato di salute, effettuati dall' I.R.C.C.S. "Saverio De Bellis"** (d'ora in avanti anche IRCCS) **per finalità amministrative e contabili.**

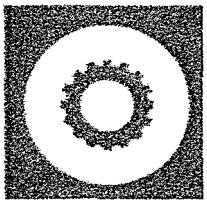
Il Titolare del trattamento è l' Azienda Ospedaliera specializzata in Gastroenterologia I.R.C.C.S. "Saverio De Bellis" con sede in Via Turi, 27 - 70013 a Castellana Grotte (Bari) , in persona del Direttore Generale pro-tempore, contattabile ai seguenti riferimenti :

Telefono: 080 4994167
email: direttoregenerale@irccsdebellis.it
pec : dirgenerale.debellis@pec.rupar.puglia.it



Il Responsabile della protezione dei dati personali è il Dott. Simone Montanaro, contattabile ai seguenti riferimenti :

Telefono 0804994162 email : simone.montanaro@irccsdebellis.it



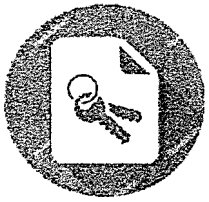
FINALITÀ DEL TRATTAMENTO

L'Ente Ospedaliero Specializzato in Gastroenterologia "Saverio de Bellis" (d'ora in avanti IRCCS) è una struttura ospedaliera ad indirizzo specialistico gastroenterologico medico e chirurgico che opera in tale campo quale Istituto di Ricovero e Cura a Carattere Scientifico di diritto pubblico.Il trattamento dei dati di tipo amministrativo e contabile da parte dell'IRCCS è effettuato per motivi di interesse pubblico rilevante nel settore della sanità pubblica ed è finalizzato a:

- Espletare tutte le attività amministrative e contabili correlate a quelle di diagnosi, assistenza e terapia sanitaria;
- Erogare attività certificatorie relative allo stato di salute;
- Svolgere attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;
- Gestire la pianificazione e controllo dei rapporti tra l'Amministrazione ed i Soggetti accreditati o Convenzionati del Servizio Sanitario Nazionale;

- Erogare attività formative professionali e attività didattiche in aula con dati trattati in forma anonima;
- Programmare i servizi di assistenza domiciliare;
- Gestire i reclami, richieste rimborsi, suggerimenti, ringraziamenti ed elogi;
- Erogare prestazioni di assistenza sanitaria in regime ALPI, in forma indiretta (ambulatoriali o in regime di degenza), presso strutture convenzionate o private autorizzate;
- Gestire le attività amministrative per il riconoscimento delle esenzioni previste per legge;
- Svolgere attività amministrative finalizzate alla fornitura di prodotti e di altri presidi sanitari;
- Gestire le attività del CUP per prenotazioni e disdette visite;
- Garantire servizi ulteriori per motivi di interesse pubblico rilevante previsti da norma di legge o di regolamento.

Per tutte le attività amministrative effettuate per motivi di interesse pubblico rilevante, come sopra elencate, non è richiesto il consenso degli interessati.



MODALITÀ DEL TRATTAMENTO DEI DATI PERSONALI

Per l'erogazione di una prestazione sanitaria, sia in regime ambulatoriale che di ricovero, Le verranno chiesti da parte degli operatori i dati personali (nome, cognome, codice fiscale, tipo di esenzione, etc.) necessari ed obbligatori per provvedere ad erogarLe e/o prenotarLe la prestazione richiesta (ad esempio assegnazione del medico di base, prenotazione della visita, ecc.). In caso di prenotazione di visita attraverso il sistema CUP o in altra occasione di contatto con l' IRCCS oltre ai sopra citati dati personali, Le potrà essere richiesto anche un numero di telefono personale, fisso o cellulare, ed un indirizzo e-mail che potranno essere utilizzati, fino a Sua diversa indicazione, per confermarLe o ricordarLe il giorno della prenotazione o per avvisarLa, anche tramite SMS, in caso di

annullamento della visita o per finalità di prevenzione e di tutela di sanità collettiva e igiene pubblica.
E' altresì attivo sul sito internet istituzionale https://www.sanita.puglia.it/web/debellis/servizi-online il servizio di visualizzazione/disdetta online delle prenotazioni che prevede anche la procedura di pagamento del ticket online.
In caso di ricovero ospedaliero, i Suoi dati anagrafici ed i dati relativi al reparto in cui Lei è ricoverato/a saranno trattati per agevolare l'accesso ai reparti di degenza da parte dei visitatori; nel caso in cui Lei non intenda renderli disponibili, può manifestare l'eventuale specifico dissenso all'atto del ricovero. I dati da Lei rilasciati all' IRCCS verranno trattati esclusivamente dal personale debitamente autorizzato e istruito dal Titolare, e saranno conservati in luogo idoneo ed appropriato, tutelandone la riservatezza, nel rispetto del segreto professionale e d'ufficio. Potranno inoltre essere trattati da imprese esterne, previamente nominate quali "Responsabili del trattamento dei dati" ai sensi dell'art. 28 del Regolamento, alle quali è affidato il compito di svolgere specifiche operazioni necessarie per garantire i servizi dell' IRCCS, nei limiti strettamente pertinenti alle finalità di cui sopra.

CONFERIMENTO DEI DATI

Ad eccezione di eventuali obblighi di legge, il conferimento dei dati personali richiesti da parte dell' IRCCS è facoltativo, ma necessario al pieno raggiungimento delle finalità sopra indicate. Fatto salvo il superiore diritto alla salute dell'individuo, l'eventuale rifiuto di conferire in tutto o in parte i dati richiesti o la successiva richiesta di cancellarli potrebbe comportare per l' IRCCS l'impossibilità di eseguire o continuare, in tutto o in parte, l'attività richiesta o comunque inerente e/o conseguente allo svolgimento delle proprie funzioni istituzionali. I dati personali indispensabili per l'erogazione delle prestazioni richieste sono forniti direttamente dall'interessato o tramite terzi legittimati (ad es. l'anagrafe unica degli assistiti della Regione Puglia).

AMBITO DI COMUNICAZIONE

I dati personali e sensibili non possono essere diffusi ma possono essere comunicati, per le finalità segnalate, a soggetti terzi, se destinatari per norma o regolamento.
Tali dati potranno essere comunicati agli enti competenti per finalità istituzionali e/o amministrative, secondo quanto previsto dalla normativa vigente: in particolare, potranno essere comunicati, solo se necessario, ai seguenti soggetti:

- ai professionisti coinvolti nella gestione clinico-assistenziale;
- agli operatori amministrativi dell'Azienda;
- ad altre Aziende Sanitarie in convenzione e alla Regione di appartenenza dell'utente;
- alla Compagnia Assicurativa dell'Azienda per la tutela della stessa e dei suoi operatori, per le ipotesi di responsabilità;
- ad altri Soggetti pubblici (ad esempio Regione, Comune, INAIL...) o privati (a cui siano affidati compiti da parte dell'Azienda) per finalità istituzionali;
- all'Autorità Giudiziaria e/o di Pubblica Sicurezza, nei casi espressamente previsti dalla legge.

Il trattamento dei dati non prevede un processo di profilazione degli assistiti in riferimento alle finalità del trattamento sopra indicate.
I dati personali potranno essere oggetto di trasferimento in paesi non appartenenti all'Unione Europea, unicamente relativamente a quelli in cui il livello di protezione è ritenuto adeguato dalla Commissione Europea ai sensi dell'art. 45 del Regolamento UE 2016/679. In qualsiasi momento potrà richiedere dettagli sui Paesi terzi, rivolgendosi al Titolare del trattamento o al Responsabile della protezione dei dati.

TEMPO DI CONSERVAZIONE

I dati personali ed idonei a rivelare lo stato di salute da Lei forniti e/o prodotti dall' IRCCS sono conservati nel rispetto delle vigenti normative in materia. Il periodo di conservazione di ciascuna tipologia di dati trattati per finalità amministrative e contabili è rilevabile dal Piano di conservazione dell'IRCCS.

I SUOI DIRITTI

In ogni momento potrà esercitare i Suoi diritti, secondo le modalità e le condizioni ivi indicate, previsti dagli articoli 15 e ss. del Regolamento (UE) 2016/679, tra cui quelli di chiedere all'IRCCS di :

- ottenere la conferma dell'esistenza o meno di dati personali che La riguardano, anche se non ancora registrati e la loro comunicazione in forma intellegibile;
- conoscere l'indicazione dell'origine dei dati personali, delle finalità e delle modalità di trattamento, nonché gli estremi identificativi dei responsabili del trattamento dei dati personali;
- conoscere l'indicazione degli estremi identificativi dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili del trattamento o persone designate e autorizzate al trattamento;
- ottenere l'aggiornamento, la rettifica ovvero l'integrazione dei dati che La riguardano;
- ottenere la cancellazione e la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
- opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta.

Lei ha altresì il diritto di :

- avanzare istanza volta a conoscere gli accessi eseguiti sui suoi dati personali all'interno del dossier sanitario;
- presentare reclamo all'Autorità Garante per la Protezione dei dati personali, in caso di illecito trattamento dei Suoi dati personali da parte dell'IRCCS, seguendo le procedure e le indicazioni pubblicate sul sito web dell'Autorità Garante www.garanteprivacy.it

I diritti di cui sopra sono esercitabili rivolgendosi direttamente al Titolare del trattamento dei dati o al Responsabile della protezione dei dati, ai contatti sopra riportati.

La versione sempre aggiornata di questa informativa è sempre rinvenibile sul sito web istituzionale all'indirizzo https://www.sanita.puglia.it/web/debellis.

INFORMAZIONI PER GLI ASSISTITI

SUL TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DELLE ATTIVITA' AMMINISTRATIVE CORRELATE ALLE PRESTAZIONI SANITARIE

1. *Perché queste informazioni ?*

Gentile Utente,

Il Codice in materia di protezione dei dati personali (D.lgs. n. 196/2003 così come modificato dal D.lgs. n. 101/2018), In osservanza del Regolamento Generale sulla Protezione dei dati (Regolamento UE 2016/679), riconosce e disciplina il diritto alla protezione dei dati personali, nel rispetto dei Suoi diritti e libertà fondamentali e della Sua dignità personale. Nella presente informativa sono riportate le informazioni relative al trattamento dei Suoi dati personali ed idonei a rivelare lo stato di salute, effettuati dall' I.R.C.C.S. "Saverio De Bellis" (d'ora in avanti anche IRCCS) per finalità amministrative e contabili.

2. *Chi decide dei mie dati personali ?*

Il Titolare del trattamento dei dati è l' Azienda Ospedaliera specializzata in Gastroenterologia I.R.C.C.S. "Saverio De Bellis" con sede in Via Turi, 27 - 70013 a Castellana Grotte (Bari) , in persona del Direttore Generale pro-tempore, contattabile ai seguenti riferimenti :
Telefono: 080 4994167
email: direttoregenerale@irccsdebellis.it
pec : direzionegenerale.debellis@pec.rupar.puglia.it

3. *Chi vigila sulla protezione dei miei dati ?*

Il Responsabile della protezione dei dati è il Dott. Simone Montanaro, contattabile ai seguenti riferimenti : Telefono 0804994162 email : simone.montanaro@irccsdebellis.it

4. *Perché sono richiesti i miei dati ?*

L'Ente Ospedaliero Specializzato in Gastroenterologia "Saverio de Bellis" (d'ora in avanti IRCCS) è una struttura ospedaliera ad indirizzo specialistico gastroenterologico medico e chirurgico che opera in tale campo quale Istituto di Ricovero e Cura a Carattere Scientifico di diritto pubblico. Il trattamento dei dati di tipo amministrativo e contabile da parte dell'IRCCS è effettuato per motivi di interesse pubblico rilevante nel settore della sanità pubblica ed è finalizzato a:

- Espletare tutte le attività amministrative e contabili correlate a quelle di diagnosi, assistenza e terapia sanitaria;
- Erogare attività certificatorie relative allo stato di salute;
- Svolgere attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;
- Gestire la pianificazione e controllo dei rapporti tra l'Amministrazione ed i Soggetti accreditati o Convenzionati del Servizio Sanitario Nazionale;
- Erogare attività formative professionali e attività didattiche in aula con dati trattati in forma anonima;
- Programmare i servizi di assistenza domiciliare;
- Gestire i reclami, richieste rimborsi, suggerimenti, ringraziamenti ed elogi;
- Erogare prestazioni di assistenza sanitaria in regime ALPI, in forma indiretta (ambulatoriali o in regime di degenza), presso strutture convenzionate o private autorizzate;
- Gestire le attività amministrative per il riconoscimento delle esenzioni previste per legge;
- Svolgere attività amministrative finalizzate alla fornitura di prodotti e di altri presidi sanitari;
- Gestire le attività del CUP per prenotazioni e disdette visite;
- Garantire servizi ulteriori per motivi di interesse pubblico rilevante previsti da norma di legge o di regolamento.

Per tutte le attività amministrative effettuate per motivi di interesse pubblico rilevante, come sopra elencate, non è richiesto il consenso degli interessati.

5. *Ci sono telecamere che mi riprendono ?*

VIDEOSORVEGLIANZA
In alcuni locali dell' IRCCS e lungo alcune aree perimetrali è attivo un sistema di videosorveglianza per ragioni di tutela della salute e sicurezza degli assistiti, dei visitatori e del personale nonché del patrimonio aziendale, adeguatamente segnalato da appositi cartelli informativi e gestito nel pieno rispetto di quanto stabilito nel Provvedimento in materia di videosorveglianza dell'8 aprile 2010 dell'Autorità Garante per la protezione dei dati personali ed in osservanza del Regolamento UE 2016/679. Per richiedere l'accesso alle sue immagini potrà inviare una richiesta direttamente al Titolare del trattamento oppure al Responsabile della protezione dei dati personali, ai contatti sopra indicati.

6. *Sono obbligato a fornire i dati ?*

CONFERIMENTO E FONTE DEI DATI

Il conferimento dei dati personali richiesti da parte dell' IRCCS è necessario al pieno raggiungimento delle finalità sopra indicate. Fatto salvo il superiore diritto alla salute dell'individuo, l'eventuale rifiuto di conferire in tutto o in parte i dati richiesti potrebbe comportare per l'IRCCS l'impossibilità di eseguire o continuare, in tutto o in parte, l'attività richiesta di diagnosi, assistenza e terapia sanitaria . I dati personali indispensabili per l'erogazione delle prestazioni richieste sono forniti direttamente dall'interessato o tramite terzi legittimati (ad es. l'anagrafe unica degli assistiti della Regione Puglia).

7. *Chi potrà conoscere i miei dati ?*

AMBITO DI COMUNICAZIONE

I dati personali e sensibili non possono essere diffusi ma possono essere comunicati, per le finalità segnalate, a soggetti terzi, se destinatari per norma o regolamento.
Tali dati potranno essere comunicati agli enti competenti per finalità istituzionali e/o amministrative, secondo quanto previsto dalla normativa vigente: in particolare, potranno essere comunicati, solo se necessario, ai seguenti soggetti: ai professionisti coinvolti nella gestione clinico-assistenziale;
agli operatori amministrativi dell'IRCCS; ad altre Aziende Sanitarie e Associazioni in convenzione e alla Regione di appartenenza dell'utente; alla Compagnia Assicurativa dell'IRCCS per la tutela della stessa e dei suoi operatori, per le ipotesi di responsabilità; ad altri Soggetti pubblici (ad esempio Regione, Comune, INAIL...) o privati (a cui siano affidati compiti da parte dell'IRCCS) per finalità istituzionali di rilevante interesse pubblico; all'Autorità Giudiziaria e/o di Pubblica Sicurezza, nei casi espressamente previsti dalla legge.
Il trattamento dei dati può prevedere, in casi particolari, un processo di profilazione degli interessati in riferimento alle finalità del trattamento sopra indicate.
I dati personali potranno essere oggetto di trasferimento in paesi non appartenenti all'Unione Europea, unicamente relativamente a quelli in cui il livello di protezione è ritenuto adeguato dalla Commissione Europea ai sensi dell'art. 45 del Regolamento UE 2016/679. In qualsiasi momento potrà richiedere dettagli sui Paesi terzi, rivolgendosi al Titolare del trattamento o al Responsabile della protezione dei dati.

8. *Per quanto tempo sono conservati i miei dati ?*

TEMPO DI CONSERVAZIONE
I dati personali ed idonei a rivelare lo stato di salute da Lei forniti c/o prodotti dall' IRCCS sono conservati nel rispetto delle vigenti normative in materia. In particolare, i dati relativi a ciascun episodio di ricovero, raccolti nella relativa cartella clinica (cartacea o elettronica), saranno conservati a tempo indeterminato. Le restanti tipologie di trattamento dati che l' IRCCS può effettuare e il periodo di conservazione di ciascuna tipologia di dati sono indicati dal Piano di conservazione dell'IRCCS.

9. *Cosa è il Dossier Sanitario elettronico ?*

DOSSIER SANITARIO ELETTRONICO

I Suoi dati personali potranno essere trattati, previo suo consenso, tramite un Dossier Sanitario Elettronico (DSE) ossia uno strumento informatizzato di raccolta di dati sanitari in formato elettronico, contenente diverse informazioni inerenti il Suo stato di salute o di colui che rappresenta legalmente, relative a eventi clinici presenti e pregressi, raccolte dall'IRCCS. Le informazioni di dettaglio sul Dossier Sanitario sono disponibili sul sito internet istituzionale nell'apposita sezione Privacy.

10. *Cosa è il Fascicolo Sanitario elettronico ?*

FASCICOLO SANITARIO ELETTRONICO

Il Fascicolo Sanitario Elettronico (FSE) è l'insieme di dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, che riguardano Lei o colui che rappresenta legalmente. Il FSE dei cittadini pugliesi è accessibile attraverso il Portale Regionale della Salute, la piattaforma unica di accesso ai servizi sanitari on line della Regione Puglia. Per maggiori informazioni si rinvia all'indirizzo web https://www.sanita.puglia.it/infofse.

11. *Quali sono i miei diritti ?*

I DIRITTI DELL'ASSISTITO
In ogni momento Lei potrà esercitare i diritti previsti dagli articoli 15 e ss. del Regolamento (UE) 2016/679, tra cui quelli di chiedere all'IRCCS di :

- **ottenere la conferma dell'esistenza o meno di dati personali che La riguardano;**
- **ottenere l'aggiornamento, la rettifica ovvero l'integrazione dei dati che La riguardano;**
- ottenere la limitazione dei dati trattati;
- opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta.
- presentare reclamo all'Autorità Garante per la Protezione dei dati personali, in caso di illecito trattamento dei Suoi dati personali da parte dell'IRCCS, seguendo le procedure e le indicazioni pubblicate sul sito web dell'Autorità Garante (www.garanteprivacy.it).

A chi posso rivolgermi ?

I diritti di cui sopra sono esercitabili rivolgendosi direttamente al Titolare del trattamento dei dati o al Responsabile della protezione dei dati, ai contatti sopra riportati (p.ti 2 e 3).
I modelli per l'esercizio dei diritti nonché le politiche aziendali in materia di protezione dei dati personali sono reperibili sul sito web aziendale all'indirizzo https://www.sanita.puglia.it/web/debellis nell'apposita sezione "Privacy".

ALL. N. 6 ALLA DDG
N° 49 DEL 18 GEN. 2019

ALLEGATO_6-Modulo-CONSENSO-ASSISTITI_GDPR_2018

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI DA PARTE DEGLI ASSISTITI IN DEGENZA

Consenso acquisito secondo le disposizioni del Codice in materia di protezione dei dati personali (D.lgs. n. 196/2003 così come modificato dal D.lgs. n. 101/2018) ed in osservanza del Regolamento Generale sulla Protezione dei dati (UE) 2016/679

Io sottoscritto (nome e cognome).....nato a ..... il ..... / ..... / ..... codice fiscale.....residente a (Comune, Prov.) ..... via (indirizzo) .....

per sé ☐

oppure
Consapevole che le dichiarazioni non veritiere sono punite dalla legge, sotto mia responsabilità dichiaro

in qualità di: ☐esercente responsabilità genitoriale ☐prossimo congiunto ☐familiare

☐convivente o unito civilmente ☐legale rappresentante ☐fiduciario (L. 219/2017)

☐responsabile della struttura presso cui dimora l'interessato

DI (nome e cognome).....nato a

..... il ..... / ..... / ..... codice fiscale.....residente

a (Comune, Prov.) ..... via (indirizzo) .....

DICHIARO DI AVER LETTO E COMPRESO le informazioni sul trattamento dei dati personali rese dall'IRCCS S. de Bellis e dopo essere stato informato dei diritti a me riconosciuti, ai sensi degli artt. 15 e seguenti del Regolamento Generale sulla protezione dei dati

PRESTO IL CONSENSO alla comunicazione, in ordine allo STATO DI SALUTE, alle sotto indicate persone:

☐a nessuno ☐al coniuge/convivente ☐altro .....
[indicare nome/cognome] ... .

PRESTO IL CONSENSO alla comunicazione della mia PRESENZA IN REPARTO a:

☐ chiunque lo richieda ☐ nessuno

PRESTO IL CONSENSO all'utilizzo dei dati personali per scopi di RICERCA scientifica in campo medico, biomedico ed epidemiologico

SI ☐ NO☐

ALLEGATO_6-Modulo-CONSENSO-ASSISTITI_GDPR_2018

DOSSIER SANITARIO ELETTRONICO E FASCICOLO SANITARIO ELETTRONICO

IDENTIFICAZIONE DOSSIER SANITARIO : .....
[indicare il nome dello strumento informatico utilizzato come dossier sanitario]

ACCONSENTO ALLA COSTITUZIONE DEL DOSSIER SI ☐ NO ☐

E ALL'INSERIMENTO DI TUTTI **I DATI PRODOTTI D' ORA IN POI** SI ☐ NO ☐

ACCONSENTO ALL'INSERIMENTO **ANCHE DI TUTTI I DATI PRECEDENTI** SI ☐ NO ☐

SI RICHIEDE ☐ L'OSCURAMENTO DELL'EVENTO ☐ DE-OSCURAMENTO DELL'EVENTO

ACCONSENTO ad inserire nel Dossier Sanitario Elettronico eventuali informazioni sanitarie inerenti aborto, uso di alcool, sieropositività, atti di violenza sessuale e pedofilia, tossicodipendenza, parto in anonimato,

prestando specifico ed esplicito consenso SI ☐ NO ☐

FASCICOLO SANITARIO ELETTRONICO (FSE REGIONE PUGLIA)

ACCONSENTO ALL'ALIMENTAZIONE DEL FSE SI ☐ NO ☐

D' ORA IN POI SI ☐ NO ☐ **ANCHE DI TUTTI I DATI PRECEDENTI** SI ☐ NO ☐

SI RICHIEDE ☐ L'OSCURAMENTO DELL'EVENTO ☐ DE-OSCURAMENTO DELL'EVENTO

Data : .....

FIRMA DELL'ASSISTITO O ESERCENTE POTESTA' (firma per esteso e leggibile) :

.....

Documento di riconoscimento tipo.....

n.....rilasciato il.....

FIRMA DELL'OPERATORE CHE HA RESO L'INFORMATIVA ED ACQUISITO IL CONSENSO
(firma per esteso e leggibile) : .....

INFORMAZIONI PER GLI ASSISTITI SUL TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DELLE PRESTAZIONI SANITARIE IN REGIME DI RICOVERO E AMBULATORIALE

Gent.le Assistito, desideriamo informarLa in merito al trattamento dei dati che Lei ci fornirà al fine di consentirLe di esprimere consapevolmente il consenso al loro trattamento. I dati sono le informazioni personali (es. dati anagrafici, recapito, tessera sanitaria, codice fiscale , ecc.) e particolari (es. informazioni sullo stato di salute) e sono indispensabili per l'erogazione e la gestione delle prestazioni sanitarie richieste.
Il **trattamento** dei suoi dati verrà effettuato per **attività di diagnosi, assistenza e terapia sanitaria** (come dettagliatamente specificato nell'informativa affissa nella sedi di questa Struttura e pubblicata sul sito internet all'indirizzo https://www.sanita.puglia.it/web/debellis nell'apposita sezione "Privacy") da parte dei dipendenti e di altri soggetti autorizzati che collaborano con questo Istituto, con modalità manuale ed automatizzata, anche mediante il Portale Regionale della Salute (https://www.sanita.puglia.it/web/pugliasalute/fse).
Il Titolare del trattamento dei dati è l' Azienda Ospedaliera specializzata in Gastroenterologia I.R.C.C.S. "Saverio De Bellis" (d'ora in avanti IRCCS) con sede in Via Turi, 27 - 70013 a Castellana Grotte (Bari).
I Delegati per il trattamento, designati dal Direttore Generale, sono i Direttori Sanitari delle Strutture Operative presso le quali i trattamenti sono effettuati. Il **Responsabile per la Protezione dei Dati (DPO)** è contattabile all'indirizzo email simone.montanaro@irccsdebellis.it.
L'IRCCS La informa altresì, che al fine di migliorare il processo di cura della salute, si avvale di innovativi strumenti informativi denominati **dossier sanitario e fascicolo sanitario elettronico (DS/FSE).** Per **DSE** s'intende l'insieme dei dati sanitari in formato elettronico relativi al Suo stato di salute, raccolti in occasione di eventi clinici presenti e passati presso questo IRCCS (ad es. lettere di dimissione, referti di visite ambulatoriali, radiografie etc.). Il **DSE** può essere costituito esclusivamente con il Suo consenso. Acquisito il Suo consenso informato specifico, la consultazione del DSE è consentita solo ai professionisti sanitari di questo IRCCS per il solo tempo indispensabile per espletare le operazioni di cura. In ogni caso il Suo eventuale rifiuto di far visualizzare i dati riguardanti il suo stato di salute mediante il DSE (oscuramento) non inciderà sulla possibilità di accedere alle cure mediche richieste. Sia in caso di revoca che di diniego, i Suoi dati sanitari restano comunque disponibili agli operatori della struttura che li ha prodotti e per le eventuali conservazioni per obbligo di legge, ma non saranno visibili da parte dei professionisti delle altre strutture aziendali. Il FSE dei cittadini pugliesi consente la condivisione delle informazioni dell'assistito tra diverse strutture sanitarie ed è accessibile attraverso il Portale Regionale della Salute, la piattaforma unica di accesso ai servizi sanitari on line della Regione Puglia. Per maggiori informazioni si rinvia all'indirizzo web https://www.sanita.puglia.it/infofse.

I SUOI DATI SONO AL SICURO. La conservazione della documentazione cartacea/elettronica avverrà a cura dell'Istituto per il periodo strettamente necessario al suo percorso di cura e secondo il piano di conservazione aziendale, in presenza di adeguate misure di sicurezza oggetto di continui controlli interni.
In ogni momento Lei potrà esercitare il diritto di accesso ai dati che La riguardano e potrà esercitare i Suoi diritti previsti dagli artt. 15 e seguenti del Regolamento generale sulla protezione dei dati.

MAGGIORI INFORMAZIONI in merito ai Suoi diritti e alle modalità di esercizio potranno essere richieste direttamente al **Responsabile per la Protezione dei Dati**:
Telefono 0804994162 email : simone.montanaro@irccsdebellis.it

Per **informazioni dettagliate** circa il trattamento dei dati personali si rinvia al sito internet all'indirizzo https://www.sanita.puglia.it/web/debellis nell'apposita sezione "Privacy".

ALL. N. 7 ALLA DDG
N° 17 DEL 18 GEN. 2019

ALLEGATO_7- Modello segnalazione interna data-breach

MODELLO SEGNALAZIONI INTERNE DI VIOLAZIONE DEI DATI

DATA BREACH REPORT – USO INTERNO

Destinatari principali della segnalazione interna :

- Direttore Generale
- Responsabile della protezione dei dati
- Direttore Sanitario
- Direttore Amministrativo
- Responsabile dei Servizi informatici Aziendali

Data : .....

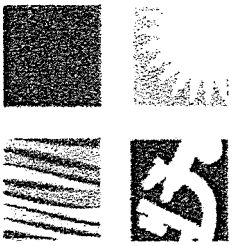
Orario : .....

UFFICIO / UNITA' INTERESSATA	
RESPONSABILE	
NOME E COGNOME DEL SEGNALANTE	
EMAIL	
TELEFONO	
BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI	
DETTAGLI TEMPORALI DELLA VIOLAZIONE (data, dal.. al , in corso)	
TIPOLOGIA DISPOSITIVO	☐ Computer ☐ Rete ☐ Dispositivo mobile ☐ File o parte di un file ☐ Strumento di backup

ALLEGATO_7- Modello segnalazione interna data-breach

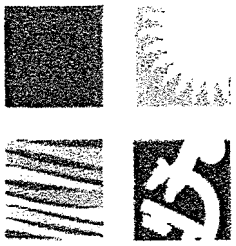
	☐ Documento cartaceo Altro : .....
TIPO VIOLAZIONE	☐ **Lettura** (presumibilmente i dati non sono stati copiati) ☐ **Copia** (i dati sono ancora presenti sui sistemi del titolare) ☐ **Alterazione** (i dati sono presenti sui sistemi ma sono stati alterati) ☐ **Cancellazione** (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione) ☐ **Furto** (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione) Altro : .....
DESCRIZIONE/UBICAZIONE DEI SISTEMI DI ELABORAZIONE E/O DI MEMORIZZAZIONE DEI DATI COINVOLTI	

QUANTI SOGGETTI SONO STATI COLPITI DALLA VIOLAZIONE DEI DATI	☐ N. persone ..... ☐ Circa persone ..... ☐ Un numero (ancora) sconosciuto di persone



ALLEGATO_7- Modello segnalazione interna data-breach

TIPOLOGIA DATI OGGETTO DI VIOLAZIONE	☐ Dati anagrafici/codice fiscale ☐ Dati di accesso e di identificazione (user name, password, SPID, CIE, altro) ☐ Dati relativi a minori ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale ☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale ☐ Dati giudiziari ☐ Copia per immagine su supporto informatico di documenti analogici ☐ Ancora sconosciuto Altro :.....
LIVELLO DI GRAVITA' DELLA VIOLAZIONE	☐ Basso/trascurabile ☐ Medio ☐ Alto ☐ Molto alto
MISURE TECNICHE ED ORGANIZZATIVE APPLICATE AI DATI OGGETTO DI VIOLAZIONE	



ALLEGATO_7- Modello segnalazione interna data-breach

Note :

.....

.....

.....

.....

.....

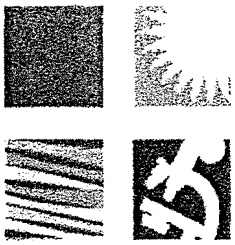
.....

ALL. N. 1 ALLA DDG
N° 19 DEL 18 GEN. 2019

IRCCS SAVERIO DE BELLIS

Regolamento interno per l'attuazione del Regolamento UE 2016/679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

INDICE

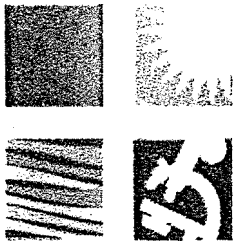


Art. 1 - Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (*General Data Protection Regulation* del 27 aprile 2016 n. 679, di seguito indicato con "**RGPD**", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati presso l'IRCCS Saverio de Bellis (*d'ora in avanti* IRCCS).

Art. 2 – Titolare del trattamento

1. L'IRCCS , rappresentato ai fini previsti dal RGPD dal Direttore Generale pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Direttore Generale può delegare le relative funzioni ai Dirigenti e/o Direttori in possesso di adeguate competenze.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.
Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa e di bilancio, previa apposita analisi preventiva della situazione in



essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

4. Il Titolare adotta misure appropriate per fornire all'interessato:

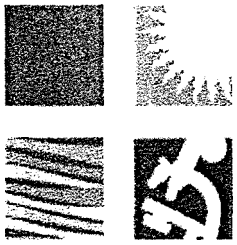
a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "VIP") ai sensi dell'art. 35, RGPD, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

6. Il Titolare, inoltre, provvede a:

   a) **designare in qualità di "Delegato interno per la protezione dei dati", tutti i Direttori/Dirigenti Responsabili pro-tempore, apicali e delle UO Complesse, Semplici e Semplici Dipartimentali in cui si articola l'organizzazione dell' IRCCS, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza,** per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;

b) **nominare il Responsabile della protezione dei dati;**
c) **nominare quale Responsabile del trattamento (ex art. 28 del GDPR) i soggetti esterni pubblici o privati affidatari di attività e servizi per conto dell'IRCCS,** relativamente alle banche dati gestite da soggetti esterni all'IRCCS in virtù di convenzioni, di contratti, o di



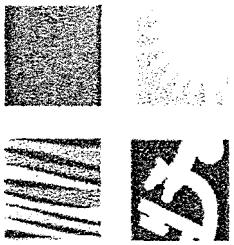
incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'IRCCS da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la **conTitolarità di cui all'art. 26 RGPD**. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in materia di protezione dei dati personali, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
8. L'IRCCS favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 3 – Finalità del trattamento

I trattamenti sono compiuti dall'IRCCS per le seguenti finalità:

- tutela della salute e dell'incolumità fisica (prestazioni di prevenzione, diagnosi, cura e riabilitazione);
- attività legate alla fornitura di beni o servizi all'utente per la salvaguardia della salute (es. fornitura di ausili e protesi);
- adempimenti amministrativi, gestionali e contabili, correlati ai compiti istituzionali dell'IRCCS e/o connessi ad obblighi di legge;
- attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;

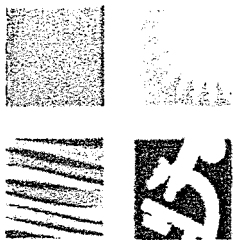


- attività epidemiologica e statistica, ricerca scientifica, didattica e genetica nel rispetto dei limiti e delle condizioni dettate dalla disciplina in materia di protezione dei dati personali
- gestione di esposti/lamentele/contenziosi ed altri adempimenti previsti da specifiche norme di legge e/o regolamento.

Art. 4 – Delegati interni e Responsabili del trattamento

1. Il Regolamento Europeo (UE) 2016/679 dispone che il trattamento dei dati possa essere effettuato esclusivamente da parte di soggetti autorizzati.
2. A tale riguardo l'IRCCS ritiene opportuno, alla luce della sua complessità organizzativa e della numerosità dei soggetti che devono essere autorizzati a trattare i dati, conferire con apposita delega una funzione di coordinamento del trattamento dei dati personali a taluni collaboratori dotati dei requisiti di esperienza, capacità e affidabilità tali da fornire idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza.

3. Ciascun Direttore/Dirigente Responsabile pro-tempore, apicale e delle UO Complesse, Semplici e Semplici Dipartimentali, è nominato dal Direttore Generale quale "Delegato interno per la protezione dei dati", in conformità al RGPD, di tutte le banche dati esistenti nell'articolazione organizzativa di rispettiva competenza. Il "Delegato interno per la protezione dei dati" deve essere in grado di offrire garanzie sufficienti in termini di conoscenza, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD. Con riferimento alle misure tecnologiche e di sicurezza informatica, adeguate al rischio insito nel trattamento dei dati, ai sensi dell'art. 32 del RGPD, ciascun "Delegato interno per la protezione dei dati" è opportunamente supportato dall'Unità Operativa Controllo di Gestione e Sistemi Informativi;
4. Ciascun "Delegato interno per la protezione dei dati" è tenuto a designare i soggetti autorizzati al trattamento dei dati, nell'area di propria competenza, mediante atto



individuale come da fac-simile in allegato al presente Regolamento (allegato n. 1- atto nomina soggetti autorizzati);

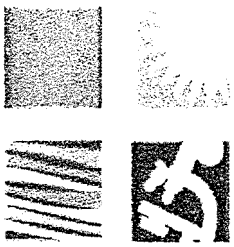
5. **Il Titolare può avvalersi, per il trattamento di dati personali e sensibili, di soggetti esterni pubblici o privati che, in qualità di Responsabili del trattamento, ai sensi dell'art. 28 del GDPR, forniscano adeguate garanzie,** stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.

6. **Gli atti** che **disciplinano il rapporto tra il Titolare ed il Responsabile (esterno) del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD**; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

7. E' consentita **la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento** per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

   Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

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



9. Il "Delegato interno per la protezione dei dati" in conformità al RGPD provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

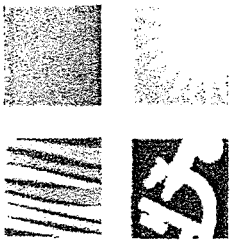
   - al supporto finalizzato all'aggiornamento del registro delle attività di trattamento svolte per conto del Titolare;

   - all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti, con il supporto dell'Unità Operativa "Controllo di Gestione e Sistemi Informativi"per quanto di competenza;

   - alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;

   - ad assistere il Titolare ed il Responsabile della protezione dei dati (RPD) nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "VIP") fornendo allo stesso ogni informazione di cui è in possesso;

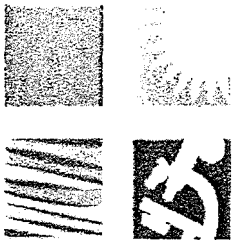
   - ad informare il Titolare ed il Responsabile della protezione dei dati (RPD), senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione all'Autorità Garante per la protezione dei dati, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.



Art. 5 – Responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è designato dal Titolare in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del Regolamento UE 2016/679, che di seguito sono elencati :

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;
c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal "Delegato interno per la protezione dei dati in conformità al RGPD";
d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (VIP) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una VIP; quale metodologia adottare nel condurre una VIP; se condurre la VIP con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la VIP sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;



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

f) (eventuale) la tenuta dei registri di cui ai successivi artt. 7 e 8;

g) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

2. Il Titolare ed il "Delegato interno per la protezione dei dati in conformità al RGPD" assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

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

a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

b) definisce un ordine di priorità nell'attività da svolgere, ovvero un piano annuale di attività, incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

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

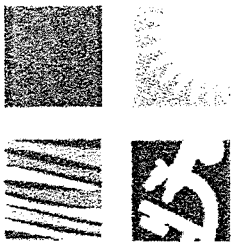
- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- il Responsabile del trattamento;
- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

5. Il RPD non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare.

Art. 6 – Gli Amministratori di Sistema

L' IRCCS, in qualità di Titolare del trattamento, individua i soggetti operanti sulla rete informatica, in qualità di Amministratori di Sistema, per ambito di operatività consentito. Nel caso di dipendenti dell' IRCCS autorizzati dal Titolare ad accedere alla rete informatica aziendale, ai computer e server con privilegi amministrativi, per fini di manutenzione ed assistenza, si procede con atto formale di nomina corredato di apposite istruzioni operative.

Nel caso di presenza di soggetti terzi (consulenti, ditte e società) autorizzati all'erogazione di servizi di assistenza sistemistica, di gestione della sicurezza informatica e monitoraggio della rete informatica, il Titolare del trattamento individua



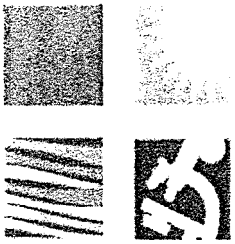
la persona giuridica in qualità di Responsabile del trattamento, ai sensi dell'art. 28 del RGPD, con la formalizzazione di un contratto tra le parti, al fine di specificare i compiti e le responsabilità di cui all'art. 4 del presente Regolamento.

Art. 7 – Informativa

L' IRCCS, in qualità di Titolare del trattamento, predispone le **informative generali** sul trattamento dei dati personali chiare e comprensibili per fornire all'interessato tutte le informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

Le informazioni da rendere all'utenza, ai sensi dell'art. 13 del RGPD, riportano almeno quanto segue :

- l'identità e i dati di contatto del titolare del trattamento;
- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo ;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo;
- 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;

- l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

Ulteriori trattamenti di dati personali, che potrebbero presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, sono effettuati, in conformità alle leggi e ai regolamenti, previa **ulteriore nota informativa** e, dove richiesto, previo rilascio del consenso dell'interessato, manifestato liberamente.

L'informativa Privacy viene resa agli interessati attraverso :

- la pubblicazione delle informazioni sul trattamento dei dati personali, sul sito internet istituzionale in apposita sezione "Privacy";
- l'affissione di appositi manifesti nelle aree ad accesso pubblico ;
- consegna delle informazioni all'utenza, in formato cartaceo o elettronico, su esplicita richiesta.

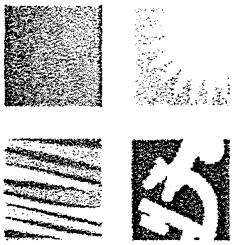
Di seguito si elencano i modelli dell'informativa privacy da utilizzare nell'ambito delle prestazioni amministrative e sanitarie offerte da questo Istituto, con relative istruzioni operative :

allegato n.2 (01-Modulo-INFORMATIVA-ASSISTITI-PRESTAZIONI-GDPR_2018) : da utilizzare nell'ambito delle prestazioni sanitarie offerte in regime di ricovero/ambulatoriale/ALPI e da stampare o inviare tramite email, su richiesta dell'Assistito o suo rappresentante legale;

allegato n.3 (POSTER-INFORMATIVA-ASSISTITI-PRESTAZIONI-GDPR_2018018) : da utilizzare nell'ambito delle prestazioni sanitarie offerte in regime di ricovero/ambulatoriale/ALPI tramite affissione di cartelli nelle sale d'attesa e nei locali di affluenza del pubblico;

allegato n.4 (ALLEGATO_4-Modulo-INFORMATIVA-ASSISTITI-AMMINISTRATIVO_GDPR_2018) : da utilizzare nell'ambito delle attività amministrative correlate alle prestazioni sanitarie (CUP, URP etc.) e da stampare o inviare tramite email, su richiesta dell'Assistito o suo rappresentante legale;

allegato n.5 (ALLEGATO_5-POSTER-INFORMATIVA-ASSISTITI-AMMINISTRATIVO_GDPR) : da utilizzare nell'ambito delle attività amministrative



correlate alle prestazioni sanitarie (CUP, URP etc.) tramite affissione di cartelli nei locali di affluenza del pubblico;

allegato n.6 (ALLEGATO_6-Modulo-CONSENSO-ASSISTITI_GDPR_2018) : da utilizzare nell'ambito delle prestazioni sanitarie offerte in regime di ricovero e da far compilare e firmare all'Assistito o suo rappresentante legale e da custodire in cartella clinica.

Art. 8 – I diritti degli interessati

Gli interessati possono contattare il Responsabile della protezione dei dati dell' IRCCS per l'esercizio dei loro diritti. L'interessato (assistito/paziente) ha il diritto di ottenere dall' IRCCS la conferma che sia o meno in corso un trattamento di dati personali che lo riguarda e in tal caso, ottenere l'accesso ai dati e alle seguenti informazioni :

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;

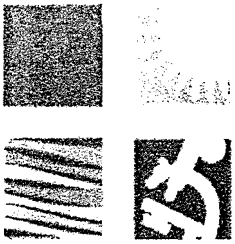
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

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

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 di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

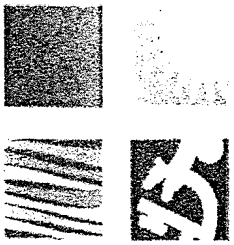
L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano e l' IRCCS si astiene dal trattarli ulteriormente salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che



prevalgono sugli interessi, diritti e libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 9 – Il diritto di accesso e il diritto alla riservatezza

L' IRCCS, in osservanza delle disposizioni vigenti in tema di riservatezza e di trasparenza, valuta anche con riguardo ad altre regolamentazioni specifiche, caso per caso la possibilità degli interessati di accedere ai documenti. L'accesso ai dati idonei a rivelare lo stato di salute o le abitudini sessuali è ammesso solo quando il diritto da tutelare, tramite istanza di accesso, è di rango almeno pari al diritto alla riservatezza, ovvero consiste in un diritto alla personalità o in un altro diritto o libertà fondamentale o inviolabile, quale ad esempio il diritto alla difesa. Ulteriori specifiche indicazioni agli operatori sono contenute negli altri regolamenti o istruzioni operative adottate dall' IRCCS.



Art. 10 – Liceità del trattamento e Consenso

I dati personali possono essere trattati soltanto :

- da parte del Titolare, dei Contitolari, dei Delegato interno per la protezione dei dati , dei soggetti autorizzati, dei Responsabili del trattamento dei dati personali e degli Amministratori di Sistema , se previsto da Legge e se sono raccolti e registrati per scopi determinati, espliciti e legittimi quando :

a) l'interessato ha prestato il consenso esplicito al trattamento dei 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;

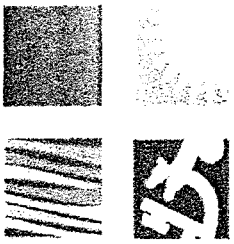
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni;

g) il trattamento è necessario per motivi di interesse pubblico rilevante che deve essere proporzionato alla finalità perseguita;

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 o conformemente al contratto con un professionista della sanità;

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;

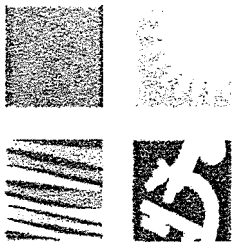


j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Nel caso in cui il trattamento dei dati personali sia basato sul rilascio del preventivo consenso da parte dell'interessato (*ad es. in ambito genetico e della medicina predittiva*), è compito dell' IRCCS dimostrare che questi abbia prestato il proprio consenso libero ed informato al trattamento dei dati personali.
Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre finalità o ulteriori specifici trattamenti di dati personali, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma facilmente accessibile e comprensibile.
Il Titolare assicura un'appropriata conservazione dei consensi espressi dagli interessati al fine anche di consentire un agevole esercizio dei diritti degli interessati.

Ulteriori trattamenti di dati personali, che potrebbero presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, sono effettuati, in conformità alle leggi e ai regolamenti, previa ulteriore nota informativa e, dove richiesto, previo rilascio del consenso manifestato liberamente dall'interessato.
Si tratta ad esempio di particolari trattamenti di dati, ad elevato rischio, effettuati nei seguenti ambiti :

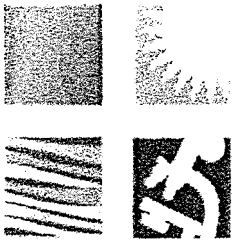
- Dossier Sanitario Elettronico e Fascicolo Sanitario Elettronico;
- Medicina c.d. predittiva;
- Sperimentazioni cliniche e genetica;
- Teleassistenza/telemedicina.



Art. 11 – Sicurezza del trattamento

1. L' IRCCS e ciascun "Delegato interno per la protezione dei dati in conformità al RGPD" mettono in atto misure tecniche ed organizzative adeguate , con il supporto dell'Unità Operativa "Controllo di Gestione e Sistemi Informativi", al fine di garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono:
   - la pseudonimizzazione;
   - la minimizzazione;
   - la cifratura dei dati personali;
   - la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
   - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
   - una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Costituiscono misure tecniche ed organizzative:

- i sistemi di autenticazione;
- sistemi di autorizzazione;
- sistemi di protezione (antivirus; firewall; antintrusione; registrazione accessi etc..);

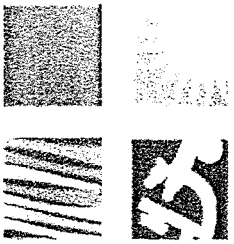


- le misure antincendio;
- sistemi di rilevazione di intrusione;
- sistemi di sorveglianza;
- sistemi di protezione con videosorveglianza;
- registrazione accessi;
- porte, armadi e contenitori dotati di serrature e ignifughi;
- sistemi di copiatura e conservazione di archivi elettronici;
- altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

4. La conformità del trattamento dei dati al RGPD, in materia di protezione dei dati personali, è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

5. L' IRCCS e ciascun "Delegato interno per la protezione dei dati" in conformità al RGPD si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali di cui è titolare l'IRCCS.

6. I nominativi ed i dati di contatto del Titolare, dei "Delegato interno per la protezione dei dati" , dei Responsabili del trattamento ex art. 28 del GDPR e del Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'IRCCS.



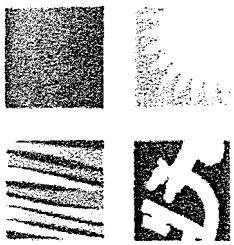
Art. 12 – Registro delle attività del trattamento

1. Il Titolare del trattamento, con il supporto del Responsabile della protezione dei dati e la collaborazione del personale tutto dell' IRCCS, predispone il Registro delle attività di trattamento recante almeno le seguenti informazioni:

a) il nome ed i dati di contatto del Titolare del trattamento dei dati ed eventualmente del Contitolare del trattamento, e del Responsabile della protezione dei dati;
b) le finalità del trattamento;
c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

2. Il Registro è tenuto dal Titolare del trattamento in formato digitale.

3. Il Titolare del trattamento può decidere di affidare al Responsabile della protezione dei dati (RPD) il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

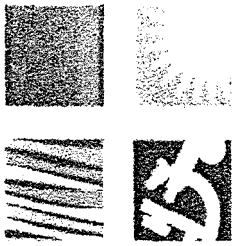


Art. 13 – Valutazione di impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (VIP - valutazione d'impatto privacy) ai sensi dell'art. 35 RGPD, considerati la
   natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La VIP è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la VIP si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, RGPD.

3. La VIP è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGPD, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
   b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
   c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;



d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGPD;

e) trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell' IRCCS, soggetti con patologie psichiatriche, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

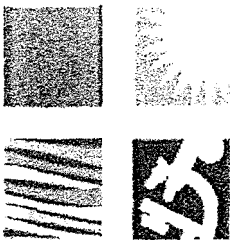
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una VIP, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una VIP.

4. Il Titolare garantisce l'effettuazione della VIP ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della VIP ad un altro soggetto, interno o esterno all'organizzazione.

   Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la VIP; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della VIP. Il RPD monitora lo svolgimento della VIP.

   Il Responsabile del trattamento deve assistere il Titolare nella conduzione della VIP



fornendo ogni informazione necessaria. Il responsabile dei Sistemi Informativi Aziendali fornisce supporto al Titolare per lo svolgimento della VIP, ove necessario.

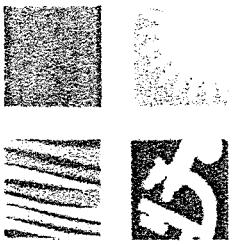
5. Il RPD può proporre lo svolgimento di una VIP in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

   Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una VIP in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La VIP non è necessaria nei casi seguenti:

   - se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGPD;
   - se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una VIP. In questo caso si possono utilizzare i risultati della VIP svolta per l'analogo trattamento;
   - se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
   - se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una VIP all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una VIP per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.



7. La VIP è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

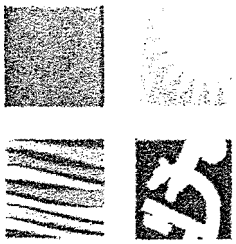
b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva dell'Autorità Garante;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione



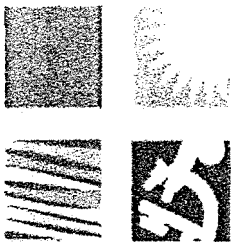
degli interessati.

9. Il Titolare deve consultare l'Autorità Garante prima di procedere al trattamento se le risultanze della VIP condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta l'Autorità Garante anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.
10. La VIP deve essere effettuata, con eventuale riesame delle valutazioni condotte, anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 14 – Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall' IRCCS.

1. In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione al Garante 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



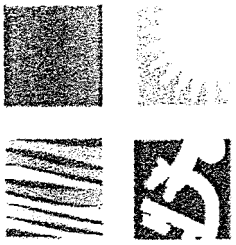
presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Ciascun "Delegato interno per la protezione dei dati" in conformità al RGPD informa il Titolare del trattamento, anche per il tramite del Responsabile della protezione dei dati, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

La notifica deve almeno:

- 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;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Il Titolare, con il supporto del Responsabile della protezione dei dati, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.



A tal fine è reso disponibile un modello per la segnalazione interna di eventuali violazioni dei dati, che si allega al presente Regolamento per farne parte integrante e sostanziale (ALLEGATO_7- Modello segnalazione interna data-breach).

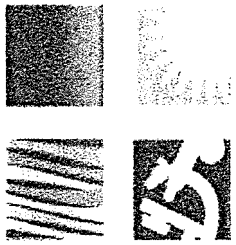
La notifica formale è effettuata dal Titolare, ove ritenuta necessaria, tramite posta elettronica certificata con l'invio del modello per la segnalazione predisposto dal Garante, all'indirizzo email databreach.pa@pec.gpdp.it.

2. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le seguenti informazioni :

   a) la natura della violazione dei dati
   b) i dati di contatto del Responsabile della protezione dei dati
   c) le possibili conseguenze della violazione
   d) le misure adottate o di cui si propone l'adozione per porvi rimedio

Non è richiesta la comunicazione all' interessato se è soddisfatta una delle seguenti condizioni:

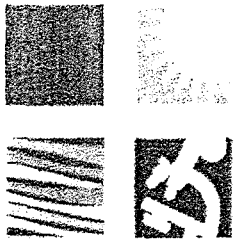
a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;



c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

3. Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui sopra è soddisfatta.

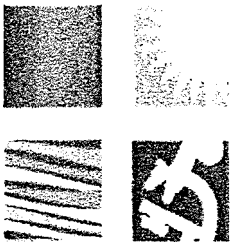
4. Nel caso di violazione dei dati personali il Titolare del trattamento procede con una valutazione complessiva dell'impatto sui diritti e libertà degli interessati in considerazione della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento.
5. I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare



mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

6. Il Titolare, con il supporto del Responsabile della protezione dei dati, verifica se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali ed informa tempestivamente l'Autorità Garante e l'interessato, se del caso.
7. A seguito valutazione preliminare della violazione, il Titolare del trattamento con il supporto del Responsabile della protezione dei dati, adotta una le seguenti azioni :

    a) se dalla violazione risulta probabile che possano derivare rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del *data-breach* al Garante, ai sensi dell'art. 33 del Regolamento UE 2016/679, secondo le previsioni di cui all'articolo 2 del presente Regolamento;
    b) se dalla violazione risulta probabile che possano derivare elevati rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del *data-breach* al Garante, ai sensi dell'art. 33 del Regolamento UE 2016/679, secondo le previsioni di cui all'articolo 2 del presente Regolamento e alla comunicazione della violazione ai soggetti interessati ai sensi dell'art. 34 del Regolamento UE 2016/679;
    c) ove non risulti probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, il Titolare del trattamento non procede con le notifiche e comunicazioni di cui ai p.ti a) e b).



Pertanto, il Titolare del trattamento è esentato dalla notifica della violazione solo se è in grado di dimostrare all'Autorità Garante che il *data-breach* non presenta rischi per i diritti e le libertà fondamentali delle persone fisiche interessate.

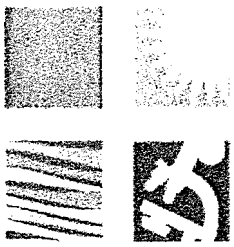
8. Ogni "Delegato interno per la protezione dei dati" (Dirigente/Responsabile di Struttura), per ambito di competenza, ha l'obbligo di segnalare senza ingiustificato ritardo, entro 24 ore, la violazione dei dati rilevata ai soggetti di seguito elencati :

   - Direttore Generale
   - Responsabile della protezione dei dati
   - Responsabile Sistemi informativi aziendali

   La segnalazione, in prima istanza, può essere effettuata in qualsiasi forma, anche per le vie brevi e successivamente formalizzata tramite invio di posta elettronica o atto interno, utilizzando il modello in allegato al presente Regolamento (allegato n. 1 - Modello segnalazione interna data-breach).
   Ai fini dell'osservanza dei tempi imposti dal Regolamento Ue 2016/679, il Titolare del trattamento dei dati, provvederà a convocare, non oltre 24 ore dalla rilevazione della violazione, una riunione con i soggetti di seguito elencati :

   - Direttore Sanitario
   - Direttore Amministrativo
   - Responsabile della protezione dei dati
   - Responsabile Sistemi informativi aziendali
   - Responsabile della Struttura interessata dal data-breach

   Il Responsabile della protezione dei dati ha facoltà di convocare altri soggetti ritenuti necessari per la valutazione della gravità della violazione dei dati.



Il Responsabile della protezione dei dati è tenuto a documentare l'intera attività istruttoria, acquisendo tutte le informazioni necessarie per la registrazione dell'evento e per la notificazione al Garante, ove necessario.

A conclusione della valutazione della violazione, il Responsabile della protezione dei dati predispone un verbale, sottoscritto da tutti i convenuti e protocollato, che sarà inoltrato al Titolare del trattamento per i conseguenti adempimenti.

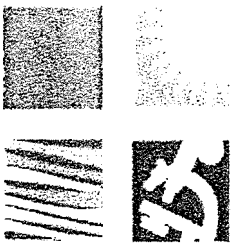
9. Il Titolare del trattamento documenta le violazioni dei dati in apposito registro elettronico da esibire in caso di accertamento ispettivo dell'Autorità.

   Il registro delle violazioni è custodito dal Responsabile della protezione dei dati con la massima diligenza e nell'osservanza del Regolamento UE 2016/679.

10. Qualora l'interessato ritenga che siano stati violati i diritti di cui gode a norma del Regolamento UE 2016/679, ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, costituiti in conformità del diritto di uno Stato membro, con obiettivi statutari di pubblico interesse, e che siano attivi nel settore della protezione dei dati personali, per proporre reclamo per suo conto al Garante, esercitare il diritto a un ricorso giurisdizionale per conto degli interessati o esercitare il diritto di ottenere il risarcimento del danno per conto degli interessati se quest'ultimo è previsto dal diritto degli Stati membri.

    Il Titolare del trattamento o il Responsabile del trattamento è tenuto a risarcire i danni cagionati ad una persona da un trattamento non conforme al Regolamento UE 2016/679 ma è esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

    La violazione delle disposizioni contenute nel Regolamento 2016/679 è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 di euro.



Art. 15 – Rinvio

Per quanto non espressamente previsto nel presente Regolamento si fà rinvio al Regolamento UE 679/2016 e successive regolamentazioni.

Il Titolare del trattamento si riserva di modificare e integrare il presente Regolamento, ove ritenuto necessario, anche alla luce di eventuali successive innovazioni normative o pronunciamenti dell'Autorità Garante per la protezione dei dati.

Art. 16 – Allegati

Si allega al presente Regolamento :

- ALLEGATO_1- Atto nomina soggetti autorizzati
- ALLEGATO_2-INFORMATIVA-ASSISTITI-PRESTAZIONI-GDPR_2018
- ALLEGATO_3-POSTER-INFORMATIVA-ASSISTITI-PRESTAZIONI-GDPR_2018
- ALLEGATO_4-Modulo-INFORMATIVA-ASSISTITI-AMMINISTRATIVO_GDPR_2018
- ALLEGATO_5-POSTER-INFORMATIVA-ASSISTITI-AMMINISTRATIVO_GDPR_2018
- ALLEGATO_6-Modulo-CONSENSO-ASSISTITI_GDPR_2018
- ALLEGATO_7- Modello segnalazione interna data-breach