

## **CONTENUTI NECESSARI DELL'INFORMATIVA E CONSENSO PRIVACY AL PAZIENTE NELL'AMBITO DI PROTOCOLLI DI STUDIO E RICERCA CLINICA**

A SEGUITO DELL'ENTRATA IN VIGORE IN DATA 25/05/2018 DEL  
**REGOLAMENTO UNIONE EUROPEA (UE) N. 679/2016**  
del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla  
**"PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHÉ  
ALLA LIBERA CIRCOLAZIONE DI TALI DATI"**

*noto anche come "GDPR 679/2016" - General Data Protection Regulation  
e del*

**D.Lgs. n. 196/2003** "Codice in materia di protezione dei dati personali" (c.d. **Codice della Privacy**)  
come modificato dal

**D.Lgs. n. 101/2018** "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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) entrato in vigore il 19/09/2018

### **A) INDICAZIONI DI CARATTERE GENERALE (tratte da sito del Garante Privacy)**

I principi generali in ordine al trattamento dei dati sono: **liceità, correttezza**, trasparenza delle modalità di raccolta/uso/consultazione/trattamento; i **dati personali** trattati devono **essere adeguati, pertinenti e limitati a quanto necessario per le finalità** del trattamento nell'ambito in cui sono conferiti.

Il nuovo approccio del Regolamento Unione Europea (UE) n. 679/2016 si basa sulla "responsabilizzazione" (c.d. "accountability" nell'accezione inglese) di titolari e responsabili del trattamento dei Dati, e cioè sulla necessità di adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento ai fini del contenimento del rischio del trattamento (misure quali la valutazione di impatto, registro dei trattamenti, misure di sicurezza, violazioni dei dati personali, nomina di un Responsabile della protezione dei dati – in inglese "Data Protection Officer" – RDP/DPO).

#### **I contenuti dell'informativa privacy**

I contenuti dell'informativa nel nuovo Regolamento UE n. 679/2016 sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, e le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del medesimo regolamento.

Ciò trova riscontro anche nel D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" (c.d. Codice della Privacy), come novellato dal D.Lgs. n. 101/2018, entrato in vigore il 19/09/2018.

In particolare, il titolare deve sempre specificare i dati di contatto del Responsabile della protezione dei dati-Data Protection Officer (c.d. RPD-DPO), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano Binding Corporate Rules (BCR), ovvero clausole vincolanti tra società facenti parte dello stesso gruppo d'impresa per i flussi interni di dati; sono state inserite specifiche clausole contrattuali modello, ecc.).

Il regolamento UE n. 679/2016 prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

### **Tempi dell'informativa**

Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del Regolamento UE n. 679/2016), l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione dei dati a terzi o all'interessato (NON della registrazione dei dati, diversamente da quanto prevedeva l'art. 13, comma 4, del D.Lgs. n. 196/2003 (Codice della Privacy).

### **Modalità dell'informativa**

Il Regolamento UE n. 679/2016 specifica in dettaglio le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e, per i minori, occorre prevedere informative idonee.

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online), anche se sono ammessi "altri mezzi" (quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra).

È pur vero che il consenso al trattamento non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta" per la sua validità, ma **tale modalità di fatto è altamente consigliata in quanto è la sola idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito"**. Inoltre, il titolare (art. 7.1) **DEVE** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Il Regolamento UE n. 679/2016 ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa** ( queste icone dovranno essere identiche in tutta l'Unione Europea e saranno definite prossimamente dalla Commissione europea).

Sono inoltre **parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa** anche se occorre sottolineare che **spetta al titolare**, in caso di dati personali raccolti da fonti diverse dall'interessato, **valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato**.

Per i dati sulla salute - "dati sensibili" - (art. 9 Regolamento UE n. 679/2016) il consenso al trattamento **DEVE** essere **esplicito, libero, specifico, informato, inequivocabile, manifesto**, attraverso "dichiarazione o azione positiva inequivocabile, non essendo ammesso un consenso tacito o presunto (pertanto non devono essere predisposte sulla modulistica destinata al paziente caselle pre-spuntate).

### **Indicazione operativa per studi/ricerche in corso, avviate prima dell'entrata in vigore del Regolamento UE n. 679/2016:**

È opportuno che i titolari di trattamento (Promotori e Centri Clinici) **verifichino la rispondenza delle informative** attualmente utilizzate ai criteri e contenuti prescritti dal Regolamento UE 679/2016 e dal D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" (c.d. Codice della Privacy) come modificato dal D.Lgs. n. 101/2018, con particolare riguardo ai **contenuti obbligatori** e alle **modalità di redazione**, in modo da apportare le modifiche o le integrazioni eventualmente necessarie.

Il consenso del paziente raccolto precedentemente al 25 maggio 2018, in virtù del solo D.Lgs. 30 giugno 2003 n. 196, "Codice in materia di protezione dei dati personali", resta valido se possiede tutte le caratteristiche di cui al Regolamento UE n. 679/2016; in caso contrario, è opportuno che il Ricercatore Responsabile - Principal Investigator (P.I.) si adoperi per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il

regolamento, previa notifica del Promotore (o del P.I. del Centro ove coincida con il promotore dello studio) notificando l'aggiornamento della modulistica pertinente al Comitato Etico di riferimento.

## **B) CONTENUTI NECESSARI INFORMATIVA PRIVACY**

Nel testo dell'informativa devono risultare i seguenti contenuti (*l'ordine espositivo non è vincolante*):

### **1) INQUADRAMENTO E BASE GIURIDICA DEL TRATTAMENTO**

- Citare sia il Regolamento dell'Unione Europea (UE) n. 679/2016 – dando atto che è entrato in vigore il 25/05/2018 negli ordinamenti di tutti i paesi comunitari, inclusa l'Italia, nonché il D.Lgs. n. 196/2003, come modificato dal D.Lgs. n. 101/2018.
- Dare atto che il Regolamento UE n. 679/2016 rafforza la tutela per il trattamento dei dati personali (e sensibili) di cui già al D.Lgs. n. 196/2003, che impone alle organizzazioni, tra cui anche Sponsor/Promotori e Centri Clinici, di utilizzare le informazioni personali in modo sicuro, aumentando le garanzie per gli individui interessati e specificando i diritti spettanti.
- Specificare che il Centro clinico e l'eventuale Promotore/Sponsor europeo che ha commissionato lo studio, tratteranno, in qualità entrambi di titolari autonomi, i dati personali in accordo a tali normative vigenti.
- Indicare idonea base giuridica del trattamento dei dati, cioè i fondamenti di liceità del trattamento medesimo (art. 6 del Regolamento UE n. 679/2016) che coincidono, in linea di massima, con quelli previsti dal Codice Privacy – D.Lgs. n. 196/2003 (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

### **2) DEFINIZIONI DI DATO PERSONALE, TRATTAMENTO, INTERESSATO** in linea con nuova definizione del Regolamento UE n. 679/2016, art. 4 punto 1) e punto 2) - **Dati anonimi e anonimizzati/pseudonimizzati**

**“Dato personale”** si intende qualsiasi informazione concernente una persona fisica identificata o identificabile, direttamente o anche indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo o a uno o più elementi caratteristici della sua identità fisica, fisiologica, sanitaria, genetica, psichica, economica, culturale o sociale.

**“Trattamento”** si intende è qualsiasi operazione o insieme di operazioni, compiute con processi automatizzati o meno, applicate ai dati personali, o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione” (articolo 4 del Regolamento UE 679/2016).

**“Interessato”** è la persona fisica o giuridica, a cui si riferiscono i dati soggetti al trattamento.

Nell'ambito della ricerca e sperimentazione clinica, oltre ai dati identificativi del soggetto partecipante (informazioni come il nome-cognome / iniziali, età, data nascita, codice fiscale, codice identificativo assegnato nell'ambito di uno studio sperimentale,...), sono particolarmente rilevanti per il Promotore/Sponsor i dati sulla salute/clinici (rientranti nella categoria di **“dati sensibili”** già definiti dal Decreto Legislativo n. 196/2003), che sono le informazioni medico-sanitarie, sia preesistenti alla partecipazione allo studio, che raccolte durante lo studio, desumibili da cartelle cliniche, immagini medico-

diagnostiche, indagini ematochimiche di laboratorio, dossier sanitario elettronico del paziente e/o altre piattaforme e/o banche dati in uso alle strutture sanitarie, nonché campioni biologici, etc..).

Il Regolamento UE n. 679/2016 non distingue le sottocategorie di dati personali, comprendendo l'accezione tutte le tipologie già definite dal D.Lgs. n. 196/2003 (Codice Privacy).

#### **“Dati Anonimizzati/Pseudonimizzati e Dati Anonimi”**

Il promotore/Sponsor ed la Struttura presso cui si svolge lo studio in genere trattano dati anonimizzati.

Dato **anonimizzato/pseudonimizzato** è quel dato che permette il collegamento dei dati raccolti nell'ambito dello studio all'identità del paziente al solo medico sperimentatore principale ed al personale collaboratore autorizzato, in quanto al momento della registrazione dei dati dell'interessato che ha acconsentito, viene assegnato al partecipante allo studio un codice speciale anonimo ed univoco (ad es. un n. cronologico, o un codice alfanumerico, spesso generato automaticamente da un sistema informatico) che lo identificherà per tutta la durata dello studio e nei campioni biologici eventuali (“pseudonimizzazione”).

L'utilizzo di questa tecnica di cifratura permette di conservare e trattare le informazioni dell'interessato in una forma tale che ne impedisca l'identificazione a qualunque persona esterna al Centro Clinico (Dati Anonimizzati/Pseudonimizzati), ed è una delle misure previste dal Regolamento UE n. 679/2016 per garantire un livello di sicurezza adeguato al rischio insito nel trattamento dei dati; solo il medico dello studio ed il personale autorizzato è in grado di collegare il codice al nominativo del partecipante.

Il trattamento di dati anonimizzati necessita di consenso specifico dell'interessato.

Dati completamente **anonimi** sono invece quelli che non permettono più in alcun modo di risalire all'identità del soggetto cui si riferiscono, e pertanto perdono la loro caratteristica di “dati personali”, non sono più considerati “Dati personali” e possono essere utilizzati e divulgati a scopo di ricerca e condivisi con altri soggetti diversi dal promotore, incluse Autorità Sanitarie e ricercatori esterni autorizzati, per studi futuri e/o ricerche sulla patologia e trattamenti sanitari, oppure per aiutare a predire come gli individui possano rispondere a un trattamento in studi futuri o per comprendere meglio questa o altre malattie.

Il dato anonimo non necessita di specifico ed ulteriore consenso dell'interessato.

### **3) NATURA DEL CONFERIMENTO DEI DATI E CONSEGUENZE IN CASO DI EVENTUALE RIFIUTO:**

Il consenso al trattamento è libero e facoltativo, del tutto volontario, nel senso che l'interessato può decidere di fornire o meno le informazioni, ma il mancato conferimento del consenso nell'ambito della sperimentazione o ricerca impedisce la partecipazione allo studio medesimo (per i partecipanti allo studio il conferimento dei dati è *obbligatorio*).

Specificare le *Conseguenze del mancato consenso* – Se il paziente deciderà di non prestare il consenso alla raccolta dei propri dati nella sperimentazione, e cioè:

- NON verrà raccolta alcuna informazione;
- Ciò NON pregiudicherà la possibilità e l'accesso a tutte le cure necessarie del caso, né precluderà di accedere ai dati relativi alle prestazioni/cure istituzionali rese nell'ambito della ordinaria cura ed assistenza sanitaria;
- NON incorrerà in alcuna sanzione

Dalla modulistica destinata al paziente deve risultare che Il consenso è liberamente prestato, specifico, informato, esplicito ed inequivocabile.

#### 4) MODALITÀ DEL TRATTAMENTO/ FINALITÀ - Come sono utilizzati i dati personali in una sperimentazione / ricerca clinica

SPECIFICARE che:

- Il trattamento dei dati potrà essere effettuato (secondo i casi) sia su supporti di tipo cartaceo, che con strumenti elettronici (modalità informatizzata/automatizzata – c.d. “profilazione”), ad esempio tramite computer, tablet, altre tecnologie informatiche /applicazioni e software...).
- I Centri Clinici e lo sponsor/promotore si impegnano a prevedere idonee misure di sicurezza di tipo tecnico e organizzativo, a garanzia della riservatezza dell’identità e dei dati, cioè per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.
- Il medico del centro e il personale collaboratore autorizzato, al momento della registrazione dei dati del paziente che ha acconsentito, assegnerà al partecipante allo studio un codice speciale anonimo ed univoco che identificherà il paziente nello studio e nei campioni biologici eventuali (ad es. un cronologico, o un codice alfanumerico) al fine di non rendere identificabile da qualunque persona esterna il paziente medesimo (“pseudonimizzazione”).
- Saranno raccolti solo i dati strettamente necessari e proporzionali all’oggetto ed alle finalità dello studio/ricerca e saranno gestiti e analizzati dal Centro Clinico e dallo Sponsor/Promotore in forma pseudonimizzata e aggregata (cioè insieme ai dati degli altri partecipanti allo studio, o a studi affini) per valutarne il corretto svolgimento, (per es. controlli di qualità, monitoraggio, auditing), per valutare se il trattamento oggetto di studio è sicuro ed efficace; per comprendere gli effetti del farmaco/trattamento (se applicabile) o gli aspetti biologici/clinici relativi alla malattia/condizione in studio.
- I dati trasmessi dal Centro Clinico al Promotore sono in genere pseudonimizzati, ovvero non in grado di identificare il paziente.
- I titolari del trattamento dei Suoi Dati si impegnano inoltre a diffondere i dati relativi alla partecipazione allo studio solo in forma rigorosamente anonima ovvero aggregata, ad esempio in pubblicazioni scientifiche, statistiche e convegni scientifici nell’ambito dello studio o ad altri ad esso associati, senza che si possa ricondurre il dato alla Sua persona.
- È possibile che anche i rappresentanti autorizzati dallo Sponsor e le società esterne che eseguono per conto dello sponsor il monitoraggio e la verifica dello studio, il Comitato Etico di riferimento e le autorità sanitarie italiane e straniere potranno conoscere i dati.
- Se le finalità del trattamento dovessero cambiare, l’interessato verrà tempestivamente informato, prima di procedere al trattamento ulteriore di dati.

#### **Esonero dall'informativa**

Sono parzialmente diversi i requisiti che il Regolamento UE n. 679/2016 fissa per l'esonero dall'informativa (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo), anche se occorre sottolineare che **spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato** (si veda art. 14, paragrafo 5, lettera b) ).

#### 5) CHI HA ACCESSO AI DATI - come sono conservati e mantenuti i dati personali

Elencare soggetti coinvolti nel trattamento:

- Medico sperimentatore – collaboratori (staff medico-sanitario / altro personale della struttura)

Contenuti necessari informativa e consenso al trattamento dati  
dopo l’entrata in vigore del Regolamento UE n. 679/2016

v. 1 del 19/09/2018

- Promotore /ricercatori e staff del promotore (monitors, auditors, personale autorizzato e delegato ad es. Organizzazioni di Ricerca a Contratto, *Clinical Research Organization* - c.d. C.R.O. )
- Ricercatori e staff dedicati allo studio, delegati ed autorizzati da promotore/Centro clinico
- Comitato etico di riferimento per lo studio
- Autorità regolatorie e/o altre Autorità ad es. per la vigilanza su farmaci e/o sperimentazioni ove applicabile
- Compagnie Assicurative per la responsabilità civile verso terzi per i danni da conduzione di studi/ricerca
- Altre terze parti, anche di altre giurisdizioni (fuori UE)\*- *si veda oltre, punto 6).*

Specificare altresì che :

- Tutti i soggetti sopra elencati mantengono i Dati Personali confidenziali, e si impegnano a garantirne la protezione e la sicurezza (In particolare, in Italia il medico sperimentatore ed il suo staff sono tenuti al segreto professionale, cioè hanno obbligo di segretezza e confidenzialità, a pena responsabilità disciplinare, penale e civile).
- I dati personali sono inseriti in banche dati sicure, gestite da promotore o altre aziende che collaborano (C.R.O. /partners .. ).
- Il contratto tra sponsor e centro clinico prevederà segnatamente garanzie e sistemi tecnici adottati in concreto a tutela privacy.

Quanto al periodo di conservazione:

- indicare esplicitamente il periodo di conservazione previsto presso il centro dal termine dello studio o, se non è possibile, i criteri utilizzati per definire tale periodo;

*ovvero, ove non previsto,*

- specificare che il trattamento dei dati personali avverrà per il tempo necessario e non superiore a conseguire gli scopi per cui le informazioni personali sono state raccolte (studi clinici) in relazione all'obbligo di conservazione previsto per legge dalla normativa italiana vigente sugli studi clinici (ad oggi, almeno 7 anni dal termine dello studio – D.Lgs. 200/2007 – art. 18) e comunque entro, e non oltre, 25 anni dalla loro raccolta (Regolamento UE 679/2016).

## **6) TRASFERIBILITÀ DEI DATI ALL'ESTERO – Indicazione della possibilità**

Ove Sponsor/promotori abbiano sede legale oppure sede/i staccate oppure partners o affiliati societari in Svizzera o in Paesi fuori dall'Area Economica Europea (EEA), o in altri Paesi quali, ad esempio, gli Stati Uniti d'America, indicare che è possibile che i Dati vengano trasferiti fuori UE, e che in tali Paesi la normativa in materia di privacy potrebbe non offrire lo stesso livello di protezione rispetto all'Italia.

Al paziente dovrebbe essere lasciata la scelta di autorizzare o meno il trasferimento dati fuori UE; ove non fosse possibile:

- Indicare in ogni caso se si tratta di un Paese terzo giudicato adeguato dalla Commissione europea, ovvero se si utilizzano Binding Corporate Rules (BCR), che sono clausole vincolanti tra società facenti parte dello stesso gruppo d'impresa per i flussi interni di dati, ovvero se sono inserite specifiche clausole contrattuali modello tra le parti coinvolte, etc...

- Specificare che, ad ogni modo, il Promotore/ Sponsor garantisce che verrà mantenuto comunque, anche in tal caso, lo standard di confidenzialità di cui alla informativa/consenso consegnata al paziente.

Attualmente NON è più richiesto il requisito dell'autorizzazione nazionale per trasferire dati fuori UE- ciò significa che il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del Regolamento UE n. 679/2016, potrà avere inizio senza attendere l'autorizzazione nazionale del Garante.

**7) INDICAZIONE DEI TITOLARI DEL TRATTAMENTO E RESPONSABILI DELLA PROTEZIONE DEI DATI PERSONALI E RELATIVE FINALITÀ , ED ALTRI DATI DI CONTATTO (può essere utilizzato testo libero ovvero una tabella sinottica)**

Specificare che il centro ed il promotore assumono entrambi il ruolo di titolari autonomi del trattamento in riferimento ai dati dello studio.

Indicare i titolari del trattamento dei dati, Responsabile/i designato/i dal Titolare ai sensi dell'articolo 39 del Regolamento UE 679/2016, nonché le persone fisiche e dati di contatto per domande o per esercitare tutti i diritti dell'interessato in materia, sia riferiti al promotore/sponsor che al Centro clinico, ed alle loro organizzazioni.

<b>PROMOTORE/SPONSOR</b>				
<b>Titolare</b>	Nome-cognome	sede	Recapito tel	e-mail /PEC
<b>Rappresentante del Titolare per l'Unione Europea</b>	Nome-cognome	sede	Recapito tel	e-mail /PEC
<i>(Eventuale)</i> <b>Clinical Research Organization</b> <i>(se lo sponsor ha nominato la C.R.O. come suo rappresentante ai fini dell'attuazione norme in materia di privacy e trattamento dei dati)</i>	Nome-cognome	sede	Recapito tel	e-mail /PEC
<b>Responsabile della protezione dei dati</b> (Data Protection Officer – c.d. RPD-DPO)	Nome-cognome	sede	Recapito tel	e-mail /PEC
<b>Altri</b>	Nome-cognome	sede	Recapito tel	e-mail /PEC

<b>CENTRO CLINICO</b>				
<b>Titolare</b> (Legale rappresentante Direttore Generale/Commissario )	Nome-cognome	sede	Recapito tel	e-mail /PEC
<b>Soggetti delegati e addetti</b> in base alla organizzazione (P.I./Staff...)	Nome-cognome	sede	Recapito tel	e-mail /PEC
<b>Responsabile della Protezione dei dati</b> (Data Protection Officer)	Nome-cognome	sede	Recapito tel	e-mail /PEC

– c.d. RPD-DPO)				
<b>Altri</b> - persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, 10, del Regolamento UE 679/2016 )  <i>NON vi è più la figura dell'incaricato al trattamento</i>	Nome-cognome	sede	Recapito tel	e-mail /PEC

## 8) SPECIFICI DIRITTI DELL'INTERESSATO RIGUARDO AI DATI PERSONALI E SENSIBILI

Elencare i diritti spettanti all'interessato in materia di trattamento dati , con sintetica indicazione del contenuto (artt. 15-22 del Regolamento UE n. 679/2016):

[diritti di **accesso, rettifica/correzione, cancellazione (OBLIO) , limitazione, opposizione, portabilità** (= trasferire i dati da un titolare ad un altro, ad es. per trasferimento da un centro clinico ad un altro)]

- il diritto di **accesso** dell'interessato (articolo 15) "L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle informazioni" - i titolari possono consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali
- il diritto di **rettifica** (articolo 16) "L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa";
- il diritto alla **cancellazione** (diritto all'**oblio**) (articolo 17) "L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano e il titolare ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali.
- il diritto alla **portabilità** dei dati (articolo 20) "L'interessato ha diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento – (il titolare deve essere in grado di trasmettere direttamente i dati ad un altro titolare indicato dall'interessato, se tecnicamente possibile)
- il diritto di **opposizione** (articolo 21) "L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano".

Per la cancellazione, specificare se la revoca all'autorizzazione al trattamento dei dati vale sin dall'origine, e cioè già al momento dell'adesione allo studio con relativo consenso al trattamento, ovvero se si inibisce il trattamento solo dal momento della revoca del consenso).

Sono ammesse deroghe ai diritti riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23, nonché di altri articoli relativi ad ambiti specifici.

Specificare:

- che talvolta nel corso dello studio potrebbe accadere che all'interessato venga temporaneamente limitato l'accesso ai suoi dati per proteggere la validità dello studio stesso (ad es. per l'assegnazione ad un braccio di trattamento/placebo), fermo restando che al termine dello studio TUTTI i dati saranno resi disponibili;
- per l'esercizio dei diritti ci si può rivolgere al Medico Responsabile dello studio, al DPO Aziendale o agli altri soggetti di cui al **punto 7)**;
- Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), di un mese, estendibile fino a tre mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego (motivato);

- l'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni. Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) - (art. 12.5 del Regolamento UE n. 679/2016 ), ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti;
- il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (*si vedano, in particolare, art. 11, paragrafo 2 e art. 12, paragrafo 6*);
- Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (*art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3*);
- La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

### **9) In particolare, il DIRITTO AL RECLAMO dell'interessato**

Tra i diritti dell'interessato, menzionare esplicitamente che nel caso in cui ritenga che siano stati violati i diritti in materia di privacy, vi è la possibilità di presentare reclami e contestazioni alle autorità competenti, ai sensi dell'art. 77 del Regolamento UE n. 679/2016 e degli artt. da 141 a 144 del D.Lgs. n. 196/2003, al titolare del trattamento del centro Clinico, in persona del legale Rappresentante (Direttore Generale del Centro Clinico)/DPO, e/o alla autorità di controllo in materia di dati personali.

In Italia, l'Autorità di controllo è:

#### **Autorità Garante Nazionale per la Protezione dei Dati Personali (c.d. "Garante Privacy" )**

Il reclamo potrà essere fatto secondo le modalità indicate sul sito internet del Garante accessibile all'indirizzo: [www.garanteprivacy.it](http://www.garanteprivacy.it) – indirizzo Piazza di Monte Citorio 121 – 00186 ROMA – e-mail: [garante@gpdp.it](mailto:garante@gpdp.it) fax (+39) 06.69677.3785, citando il codice di protocollo dello studio,

È possibile anche fare reclamo all'autorità europea (<http://ec.europa.eu>).

Resta la possibilità di accedere alle forme di tutela Giudiziaria ordinaria, civile e penale per la materia della protezione dei dati personali (art. 82 del Regolamento UE 679/2016 e artt. da 152 a 154 ter del D.Lgs. 196/2003).

Il reclamo al garante tuttavia non può essere proposto se già avviato ricorso all'Autorità Giudiziaria.

### **10) In particolare, il DIRITTO DI REVOCA del consenso al trattamento dei dati**

Tra i diritti dell'interessato, menzionare esplicitamente che vi è la possibilità, in ogni momento e senza fornire alcuna giustificazione, di revoca del consenso alla raccolta e al trattamento dei dati personali, in particolare le informazioni sulla salute.

Infatti ogni paziente ha il diritto di interrompere la partecipazione allo studio, e da quel momento in poi non saranno raccolti ulteriori dati. Potrà essere autorizzata dal paziente l'utilizzazione di quelli già raccolti e trattati, fermo restando che sono sempre utilizzabili per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; in caso contrario, i dati non più necessari saranno cancellati immediatamente.

I dati conservati fino a revoca possono essere ancora utilizzati laddove ciò sia necessario per:

- ✓ determinare gli effetti dei medicinali sperimentali,

- ✓ assicurare che interessi legittimi Suoi (di Vostro/a figlio/a) non siano pregiudicati,
- ✓ soddisfare l'obbligo di presentare documenti di approvazione completi.

L'utilizzo di quanto già trattato/raccolto è sempre possibile laddove ciò sia necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

## 11) NOTIFICA DELLE VIOLAZIONI DI DATI PERSONALI - c.d. Data Breach

Indicare al Paziente che, considerato il rischio potenziale di eventi di intrusione nei sistemi tecnologici, è stato introdotto dal Regolamento UE n. 679/2016 (artt. 33 e 34 del Regolamento UE n. 679/2016) un processo obbligatorio per tutte le pubbliche amministrazioni, comprese quindi anche quelle sanitarie, denominato "Data breach".

Questo processo obbliga le amministrazioni a comunicare il tipo di intrusione, il danno (cioè la quantità e la tipologia di dati personali oggetto dell'intrusione) e il tipo di procedure e strumenti già in essere e quelli che si intende implementare a fronte dell'avvenuta intrusione.

Tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico – hanno l'obbligo di notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

Se la probabilità di tale rischio è elevata, si dovrà informare delle violazioni anche gli interessati, sempre "senza ingiustificato ritardo"; i contenuti della notifica all'autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del regolamento UE n. 679/2016.

## 12) SANZIONI PER ILLECITO TRATTAMENTO DATI

La violazione della privacy, attraverso un trattamento illecito dei dati personali, è punita con le specifiche Sanzioni amministrative previste dall'art. 83 del Regolamento UE 679/2016, economiche e correttive irrogate dal Garante per la Protezione dei Dati Personali, tenuto conto delle circostanze concrete del singolo caso.

Anche il codice civile prevede sanzioni per i titolari del trattamento qualora si abbiano danni materiali e morali conseguenti ad uno scorretto utilizzo di dati personali, nei casi di omessa o incompleta notifica del trattamento al Garante, di inosservanza delle richieste del Garante o per l'omessa informativa ai soggetti interessati. Il trattamento dei dati è infatti "attività pericolosa" (ai sensi dell'art. 2050 Codice Civile) pertanto comporta la responsabilità civile del/i titolare/i, sanzionata cioè con l'obbligo di risarcire qualora si abbiano danni materiali e morali conseguenti ad uno scorretto utilizzo di dati personali, nonché nei casi di omessa o incompleta notifica del trattamento al Garante, di inosservanza delle richieste del Garante o per l'omessa informativa ai soggetti interessati.

*art. 2050 Codice Civile "Responsabilità per l'esercizio di attività pericolose" - Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.*

In virtù del principio di **accountability**, termine in lingua inglese utilizzato dal legislatore europeo per esprimere il concetto "responsabilizzazione", enunciato esplicitamente dal Regolamento UE n. 679/2016, tutti i titolari (e Responsabili) del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento medesimo.

Sono altresì previste specifiche sanzioni dal Codice Penale, nonché da leggi e atti aventi forza di legge vigenti nell'ordinamento italiano, anche per effetto di disposizioni UE ove la violazione costituisca illecito

penale (reati di cui agli artt. 167-172 del D.Lgs. n. 196/2003; ad esempio, è punita l'omessa adozione di misure di sicurezza, nonché l'omessa osservanza dei provvedimenti del garante e la falsità nelle dichiarazioni al Garante, la diffusione illecita su larga scala di dati personali, etc..).