

***La tutela della Privacy al triage  
(trattamento dei dati personali e sensibili)***

**Dott.ssa Assunta De Luca  
Marzo 2021**



# La normativa sul trattamento dei dati personali e sensibili - ad oggi

Decreto legislativo del 30 giugno 2003, n°196 «Codice in materia di protezione dei dati personali» che abrogava la legge sulla privacy n.675/96.

D.Lgs. n. 101 del 10 agosto 2018, **che adegua il nostro ordinamento** (Codice Privacy D.Lgs 196/03) al Regolamento n. 679/2016 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 (c.d. regolamento generale sulla protezione dei dati - **General Data Protection Regulation –GDPR**)

Documento n.9091942 del 7 marzo 2019 dell’Autorità del Garante della Privacy, che ha chiarito l’applicazione della disciplina di protezione dei dati in ambito sanitario

# INIZIATIVE ATTE A TUTELARE LA PRIVACY DELL'INTERESSATO 1



**Nomina del DPO** (Data Protection Officer - Responsabile della Protezione dei Dati-RPD; GDPR articolo 37) nelle strutture dove si trattano dati personali sensibili, quali quelli sanitari, persona deputata a verificare l'osservanza interna del regolamento.

- «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**;
- «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

# INIZIATIVE ATTE A TUTELARE LA PRIVACY DELL'INTERESSATO 2



- “**misure di sicurezza**” per la gestione delle informazioni sullo stato di salute (es. cartelle cliniche cartacee ed elettroniche, invio telematico di referti clinici, ecc.).
- 1) Principio della *privacy by design* oppure *by default* (GDPR *Articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*),
- 2) il DPIA (Data protection Impact Assessment) (GDPR *Articolo 35 Valutazione d'impatto sulla protezione dei dati*),
- 3) l'attivazione del Registro delle attività di trattamento (GDPR *Articolo 30 Registri delle attività di trattamento*) e
- 4) l'introduzione della gestione del data breach ovvero la violazione dei dati personali (GDPR *Articolo 33 Notifica di una violazione dei dati personali (data breach) all'autorità di controllo entro 72 ore*);

# INIZIATIVE ATTE A TUTELARE LA PRIVACY DELL'INTERESSATO 3



- **“misure di garanzia”**, quali, la **minimizzazione** e **pseudonimizzazione** dei dati sensibili (art. 110 bis del Codice privacy), le modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a **garantire i diritti degli interessati**, tali modalità sono stabilite in fase di progettazione della protezione in un una data struttura (GDPR *Articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*).

# DEFINIZIONE DI DATI PERSONALI RELATIVI ALLA SALUTE



## GDPR “considerando” n.35

“... tutti i **dati riguardanti lo stato di salute** dell’interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l’anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell’interessato, indipendentemente dalla **fonte**, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro”.

## GDPR “considerando” n.53

le **informazioni per finalità relative alla salute**, largamente intesa, devono essere considerate come **categorie particolari di dati personali** lasciando ai singoli stati membri di introdurre ulteriori limitazioni/condizioni per garantire una maggiore protezione.



# MODALITÀ DI TRATTAMENTO DEL DATO PERSONALE RELATIVO ALLO STATO DI SALUTE

- GDPR all'articolo 9 “Trattamento di categorie particolari di dati personali”
- D.Lgs. 101/2018 al articolo 2 septies “Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute”

**Questi dati possono essere trattati sotto la responsabilità di un professionista soggetto al segreto professionale.**

**Non è più necessario recepire il consenso da parte dell'interessato (paziente) per il trattamento dei suoi dati personali, ma risulta fondamentale che egli venga correttamente “**informato**” sulle modalità con cui il suo dato viene utilizzato.**



# MODALITÀ DI TRATTAMENTO DEL DATO PERSONALE RELATIVO ALLO STATO DI SALUTE

- Codice Privacy italiano al Capo II “Modalità particolari per informare l’interessato e per il trattamento dei dati personali»

**L’informativa deve essere fornita da tutti gli esercenti professioni sanitarie e le strutture sanitarie e socio-sanitarie tanto pubbliche quanto private, nonché gli altri soggetti pubblici operanti in ambito sanitario o della protezione e sicurezza sociale.**

**L’informativa deve essere chiara anche rispetto a trattamento di dati che riguardano: la ricerca scientifica, la teleassistenza o telemedicina ed ai servizi resi attraverso la comunicazione elettronica nonché ai fini dell’implementazione del fascicolo sanitario elettronico (FSE), dei sistemi di sorveglianza e dei registri di patologia.**



# L' informativa all'interessato (paziente)



- il GDPR (articoli 12,13, 14) e il Codice Privacy (articoli del Capo II) descrivono cosa deve contenere l' informativa ed enfatizzano l'importanza di usare un linguaggio semplice, chiaro che possa essere compreso anche da soggetti minorenni (minore di anni 16).
- **L' informativa può essere fornita oralmente e/o scritta** (scelta preferibile in quanto considerata dal Garante una modalità che rende inequivocabile ed esplicito l'aver compreso quanto riportato nell' informativa).

## **Art. 82 codice privacy - Emergenze e tutela della salute e dell'incolumità fisica**

1. Le informazioni di cui agli articoli 13 e 14 del Regolamento possono essere rese senza ritardo, successivamente alla prestazione, nel caso di emergenza sanitaria o di igiene pubblica



# La conservazione documentale e comunicazione stato di salute

L'introduzione del regolamento europeo non ha variato alcuni aspetti già esistenti:

- (1) la conservazione dei documenti sanitari con dati sensibili in luoghi con accesso controllato a cui possono accedere solo persone preventivamente autorizzate e
- (2) la comunicazione a parenti, conoscenti del paziente previo suo consenso delle sue condizioni di salute o della sua presenza nella struttura sanitaria.

# Scheda divulgativa Garante Privacy



## Trattamento di dati sulla salute in ambito sanitario ai sensi del Regolamento (UE) 2016/679

Trattare «categorie particolari di dati» in ambito sanitario è sempre vietato, tranne che per:

- a) motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri
- b) motivi di interesse pubblico nel settore della sanità pubblica (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare);
- c) finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali («finalità di cura»)

← Es: Pandemia da SarsCov2

### I trattamenti che:

- sono essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute;
- e
- sono effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza

**NON richiedono il consenso al trattamento dei dati da parte dell'interessato**

E' possibile trattare dati sanitari SOLO con il consenso dell'interessato per:

- consultazione del Fascicolo sanitario elettronico
- consegna del referto online
- utilizzo di app mediche
- fidelizzazione della clientela
- finalità promozionali o commerciali
- finalità elettorali



### TEMPI DI CONSERVAZIONE

Qualora non siano fissati da specifiche norme, spetta al titolare definirli in base alla finalità del trattamento. In ogni caso, devono essere indicati nell'informativa

### INFORMATIVA

Deve essere concisa, trasparente, intelligibile e facilmente accessibile, scritta con linguaggio semplice e chiaro

### NOMINA DI UN RPD

Obbligatoria per gli organismi pubblici (es: struttura appartenente al SSN) e nel caso di trattamenti su «larga scala» (come può avvenire per ospedali e case di cura)

### TENUTA DEL REGISTRO DEI TRATTAMENTI

E' obbligatoria



# ***ASPETTI PRATICI***

- il modulo sull'informativa al trattamento dei dati personali e il consenso alla comunicazione ai parenti/conoscenti sono strumenti a supporto della gestione del processo di comunicazione tra personale sanitario e paziente/familiare dei pazienti.
- La somministrazione della modulistica può essere fatta in pronto soccorso (dal triage alla fase di visita post triage) ed in Osservazione Breve Intensiva (OBI).



# Quali informazioni deve contenere l'informativa?

Il modulo relativo all'informativa al trattamento del dato personale deve riportare quanto richiesto dal codice privacy e dal regolamento europeo:

- Chi è il titolare del trattamento;
- Chi è il responsabile della protezione dati (Dpo - Data protection officer);
- la finalità del trattamento del dato: perché servono i dati e perché devono essere conservati;
- la base giuridica su cui si fonda il trattamento e l'interesse legittimo nel caso in cui questo costituisca la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- l'eventuale trasferimento dei dati personali in Paesi terzi e, in caso affermativo attraverso quali strumenti.



## Quali informazioni deve contenere il consenso alla comunicazione a terzi?

- deve prevedere espliciti riferimenti a chi poter rilasciare informazioni/comunicazioni circa lo stato di salute del paziente stesso.
- Le domande devono essere descritte in modo chiaro e la possibilità di risposta deve essere inequivocabile (esempio risposte chiuse: sì, no).



# Schema esemplificativo di modulo privacy

Il sottoscritto:

Cognome e Nome \_\_\_\_\_ Nato il \_\_\_\_\_ a \_\_\_\_\_

Residenza \_\_\_\_\_

proprio conto, ovvero, quale esercente la potestà genitoriale sul minore indicato

esercitando la potestà genitoriale sul minore \_\_\_\_\_

dichiara di aver compreso i contenuti dell'informativa circa il trattamento dei dati personali necessari allo svolgimento di quanto riportato dall'informativa stessa (attività di prevenzione, diagnosi, cura, riabilitazione correlate all'accesso in Pronto Soccorso e ricovero)

presta il consenso a rilasciare le informazioni sullo stato di salute, oltre che a me personalmente, alla persona specificamente indicata:

**Grado Parentela**          **Nome e**          **Cognome**  
\_\_\_\_\_  
\_\_\_\_\_

**Telefono** \_\_\_\_\_

Firma leggibile avente diritto \_\_\_\_\_



## Chi e quando somministrare l'informativa in PS?

- **TRIAGE** (amministrativi o infermieri) durante la raccolta dei dati anagrafici per codici di priorità di accesso differibili;
- **Medici di PS** (in caso di codici 2 o 1 dopo aver prestato le cure di stabilizzazione clinica).

Il personale deve informare e quindi descrivere al paziente sul significato dell'informativa prima di sottoporgli il modulo da firmare (salvo emergenza clinica).



# Il dossier sanitario



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Dossier sanitario - Domande più frequenti

## 1) Che cos'è il dossier sanitario?

Il dossier sanitario è l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, che vengono condivisi tra i professionisti sanitari che lo assistono presso un'unica struttura sanitaria (ad es. ospedale, casa di cura privata, ecc.).

L'accesso in PS con relativa presa in carico registrato nella cartella di PS può far parte di un percorso di cura interno alla struttura sanitaria e per questo va a costituire parte del dossier sanitario del paziente

## 4) Da chi può essere consultato il dossier sanitario?

Il dossier è accessibile da parte di tutti gli operatori sanitari della struttura sanitaria titolare del dossier che prenderanno in cura nel tempo l'interessato



SALUTE LAZIO  
SISTEMA SANITARIO REGIONALE



REGIONE  
LAZIO

# Il dossier sanitario



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

**Dossier sanitario - Domande più frequenti**

## **6) Il trattamento tramite dossier necessita di consenso dell'interessato?**

Sì. È necessario acquisire il consenso informato dell'interessato. Va chiarito tuttavia (e l'informativa deve precisarlo) che l'eventuale mancato consenso al trattamento mediante dossier non incide sulla possibilità di accedere alle cure mediche richieste.

## **9) Vi sono dei trattamenti per i quali occorre un consenso specifico dell'interessato?**

Sì. L'inserimento nel dossier di informazioni sottoposte a maggior tutela da parte dell'ordinamento (come ad esempio informazioni relative ad atti di violenza sessuale o pedofilia, all'infezione da HIV o all'uso di alcool o di stupefacenti) deve essere espressamente menzionato nell'informativa e sottoposto a un consenso specifico dell'interessato.

## **10) Può l'interessato chiedere di non far comparire alcune informazioni sulla propria salute all'interno del dossier sanitario?**

Sì. L'interessato può decidere di oscurare taluni dati o documenti sanitari, che dunque non saranno visibili e consultabili tramite il dossier.



**SALUTE LAZIO**  
SISTEMA SANITARIO REGIONALE



**REGIONE  
LAZIO**

# Il GDPR e la pandemia da Sars-Cov2



## FAQ - Trattamento dati nel contesto sanitario nell'ambito dell'emergenza sanitaria

Tutti i professionisti sanitari possono raccogliere le informazioni che ritengono necessarie nell'ambito delle attività di cura dei loro pazienti, ivi comprese quelle legate alla presenza di sintomi da COVID-19.

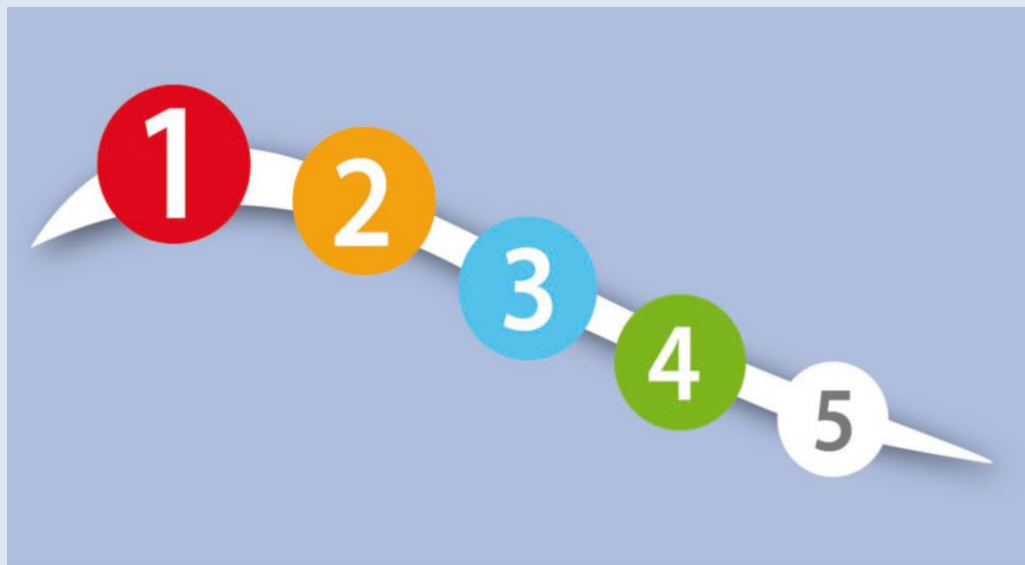
**3. È lecito che l'operatore sanitario, durante l'esecuzione di un tampone per COVID 19, chieda al paziente l'identità della persona positiva con cui ha avuto un contatto stretto?**

Si, in quanto l'operatore di sanità pubblica, al fine di determinare le misure di contenimento di contagio più opportune, è chiamato a ricostruire la filiera dei contatti stretti del soggetto risultato positivo al COVID 19.

**8. È possibile diffondere i dati identificativi delle persone positive al COVID 19 o che sono state poste in isolamento domiciliare?**

La disciplina vigente vieta la diffusione dei dati relativi alla salute. Tale divieto non è stato derogato dalla normativa d'urgenza sull'emergenza epidemiologica da Covid-19.

Pertanto, le aziende sanitarie e qualsiasi altro soggetto pubblico o privato non possono diffondere, attraverso siti web o altri canali, i nominativi dei casi accertati di Covid-19 o dei soggetti sottoposti alla misura dell'isolamento per finalità di contenimento della diffusione dell'epidemia. Solo attraverso canali istituzionali autorizzati al trattamento di dati sensibili previo consenso dell'interessato.



***La tutela della Privacy al triage  
(trattamento dei dati personali e sensibili)***

**Dott.ssa Assunta De Luca  
Marzo 2021**