GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

I TRATTAMENTI DI DATI PERSONALI PER FINALITÀ DI CURA

Cecilia Lugato
Dipartimento sanità e ricerca

11 giugno 2025

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

La domanda

Delimitazione del concetto del trattamento di dati per finalità di cura: chiarire quali sono i trattamenti compresi nell'ambito della «finalità di cura» e se tale concetto debba essere interpretato in senso restrittivo (non comprensivo di eventuali trattamenti accessori e/o ancillari alla cura in senso stretto) o se, diversamente, si possa adottare un'interpretazione più estensiva (in tal caso definendone il perimetro con particolare riguardo ai trattamenti accessori/ancillari)

Il quadro normativo di riferimento

I dati sulla salute in ambito sanitario

Artt. 5, 6 e 9 del Regolamento, in particolare il par. 4

- PER I DATI RELATIVI ALLA SALUTE
- ULTERIORI CONDIZIONI
- LIMITAZIONI

In particolare, per i dati sulla salute in ambito sanitario

Art. 75 e ss. del Codice Privacy

Art. *2-quater e septies* del Codice Privacy

Specifiche disposizioni di settore

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

DATI SULLA SALUTE

Art. 9 del RGPD

DEROGA AL DIVIETO

- **Motivo di interesse pubblico rilevante** *(Art. 9, par 2, lett. g))*
- **Sanità pubblica** *(Art. 9, par 2, lett. i))*
- **Diagnosi e cura** *(Art. 9, par 2, lett. h))*

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Eccezione al divieto di trattare dati sulla salute si applica solo al coesistere di due condizioni

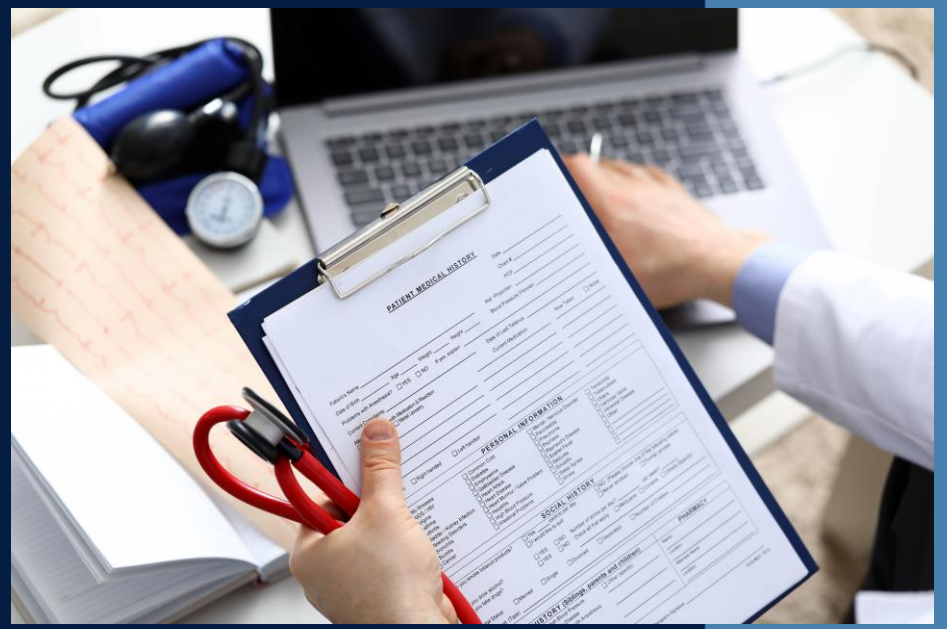
GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Provvedimento di chiarimenti in ambito sanitario
7 marzo 2019
(*doc. web n. 9091942*)

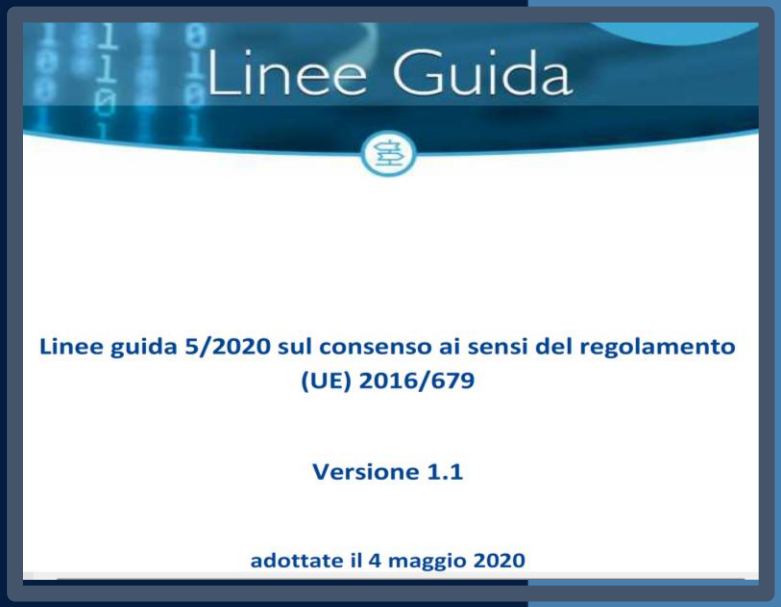
Art. 9, par. 3: soggetti ai quali si applica la deroga



Particolari casi di trattamento che invece richiedono una diversa base

CONSENSO

- *App* mediche (cfr. il Compendio del Garante del 28 marzo 2024)
- Fidelizzazione clientela
- Persone giuridiche per finalità promozionali o commerciali
- Professionisti sanitari per finalità commerciali o elettorali
- Referti *on-line* - specifica disciplina
- *Dossier* sanitario - specifica disciplina



GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Breve cenno alle app mediche

Compendio sul trattamento dei dati personali attraverso piattaforme volte a mettere in contatto i pazienti con i professionisti sanitari accessibili via web e app - marzo 2024 - *doc. web n. 9997624*

1

Le finalità e le basi giuridiche del trattamento

Tre macro tipologie di trattamenti che perseguono diverse finalità e si basano su diversi presupposti di liceità

- *trattamento dei dati degli utenti che si registrano alle piattaforme, si dati sulla salute, no finalità di cura quindi consenso*
- trattamento dei dati personali dei professionisti sanitari sulla base del contratto in essere con il gestore piattaforma
- trattamento di dati sulla salute dei pazienti per finalità di cura, art. 9, par. 2, lett. h) GDPR

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Trattamenti di dati sulla salute per finalità di cura: alcuni provvedimenti del Garante da cui trarre utili spunti

- Provvedimento del 29 settembre 2021 n. 358 (doc. web n. 9720448)
- **Provvedimento del 29 settembre 2021 n. 358 (doc. web n. 9720448)**
- **Provvedimento del 28 settembre 2023, n. 425 (doc. web n. 9946712)**
- **Tribunale Ordinario di Prato N. R.G. 1300/2023**
- **Provvedimenti del 13 febbraio 2025, nn. 81 e 82 (doc. web nn. 10107246 e 10107246) e NewsLetter del 21 marzo 2025**

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Finalità commerciale

Provvedimento del 28 settembre 2023, n. 425 (*doc. web n. 9946712*)

- il reclamante aveva segnalato che, dopo essersi sottoposto ad una visita pneumologica, aveva ricevuto dal medico una mail contenente il referto, conclusioni, diagnosi e commenti, inviata anche alla società che doveva fornire il macchinario;
- il **trattamento non è stato considerato rientrante nella "finalità di cura"**, considerato che **l'operazione** di **comunicazione non era "essenziale"** per il raggiungimento di una finalità determinata ed esplicitamente connessa **alla cura della salute**; ciò, in quanto, il paziente aveva già ricevuto l'indicazione della società alla quale, invece, lui stesso avrebbe potuto rivolgersi, ove lo avesse voluto;
- il paziente, già informato, aveva manifestato di voler provvedere quanto prima all'acquisto del macchinario, con ciò dimostrando l'intenzione di procedere autonomamente;
- l'anticipazione alla società delle informazioni dell'interessato, non sono state considerate imprescindibili per la cura, considerato che il paziente era già nelle condizioni di agire autonomamente procurandosi il macchinario.

Tribunale Ordinario di Prato
N. R.G. 1300/2023

Sulla natura del trattamento sanitario volto a finalità di cura essenziale:

«anche qualora dovesse ritenersi che la trasmissione dei dati fosse indefettibile per la più pronta "titolazione" del macchinario necessario alla cura, in alcun modo può ritenersi che la società commerciale dovesse conseguire informazioni ulteriori rispetto a quelle strettamente inerenti la patologia riscontrata.

L'invio dell'intero referto comprensivo dei dati identificativi dell'interessato è stata considerata ultronea rispetto alle specifiche finalità di cura rivendicate quale scriminante dal medico

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Finalità promozionale-commerciale

Provvedimento del 29 settembre 2021 n. 358 (*doc. web n. 9720448*)

- ✓ un medico aveva comunicato i dati personali di un suo paziente (num. cellulare), ad un consulente aziendale di alcuni prodotti dei quali il medico aveva consigliato l'assunzione
- ✓ le informazioni riguardanti il fatto che l'**interessato si era sottoposto a visita presso il medico ed era suo paziente costituiscono dati sulla salute**, sebbene non siano state indicate le motivazioni cliniche e/o la patologia del segnalante
- ✓ necessario **acquisire il consenso** per la comunicazione a terzi di informazioni, anche riguardanti la salute, qualora tale comunicazione non sia "essenziale" per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute
- ✓ nel caso in esame la comunicazione di dati sulla salute allo scopo di proporre l'acquisto di prodotti naturali, in assenza del consenso, avendo una funzione commerciale, è stata posta in violazione della disciplina in materia di protezione dei dati personali

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Cosa di intende per dato sulla salute

Gli orientamenti della Corte di Cassazione

- ✓ il fatto stesso di comunicare **l'esigenza di un trattamento sanitario** e, quindi, l'esistenza di una "malattia" in senso lato - intesa dunque come situazione che renda necessario un trattamento sanitario - **attiene a dato sulla salute**: non occorre che sia specificato di quale trattamento o di quale malattia si tratti (Cass. 28417/2023);
- ✓ il **semplice riferimento ad un'assenza dal lavoro "per malattia"** costituisce un dato personale «relativo alla salute» del soggetto cui l'informazione si riferisce (Cass. 18980/2013);
- ✓ l'**ostensione di una situazione di invalidità** sia pur genericamente indicata (Cass. 16816/2018);
- ✓ la **necessità del lavoratore di sottoporsi a "consulenza psichiatrica"** (Cass. 2367/2018);
- ✓ la indicazione della **causale del bonifico** richiesto in favore di un beneficiario dell'**indennizzo** che ha patito una **infezione per effetto di trasfusione o vaccinazione** è un dato sulla salute (Cass. 30981/2017).

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Il gestore di una farmacia commercializza, tramite una piattaforma online, medicinali la cui vendita è riservata alle farmacie, le informazioni che i clienti di tale gestore inseriscono al momento dell'ordine online dei medicinali, quali il loro nome, l'indirizzo di consegna e le informazioni necessarie all'individualizzazione dei medicinali sono dati sulla salute

Corte di Giustizia europea
Sentenza causa n. 21/23

- ✓ la nozione di «dati relativi alla salute», deve essere interpretata in senso ampio;
- ✓ consentono di trarre conclusioni sullo stato di salute di una persona identificata o identificabile **mediante un'operazione di raffronto o di deduzione, informazioni sullo stato di salute dell'interessato;**
- ✓ L'ordine effettuato sulla piattaforme implica la creazione di un nesso tra un medicinale, le sue indicazioni terapeutiche o i suoi usi, e una persona fisica identificata o identificabile da elementi quali il nome o l'indirizzo di consegna, **a prescindere dal fatto che tali informazioni riguardino tale utente o qualsiasi altra persona per la quale quest'ultimo effettua l'ordine.**

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

I RUOLI DI PROTEZIONE DEI DATI PERSONALI

Cecilia Lugato
Dipartimento sanità e ricerca

11 giugno 2025

Le domande

1) ruolo delle Regioni quando mettono a disposizione dei diversi Enti del sistema sanitario regionale piattaforme/sistemi informativi;

2) ruolo delle società *in house* che sviluppano servizi di natura tecnica (quali ad esempio accesso del cittadino tramite applicazioni ai servizi della sanità, fascicolo sanitario elettronico, prenotazioni, pagamenti, ecc.);

3) ruoli nelle aggregazioni funzionali territoriali tra medici di medicina generale/pediatri di libera scelta, ecc.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Il quadro normativo di riferimento

Articoli 24, 26, 28, 29 e considerando da 74, 75, 78, 79 e 81

Articolo *2-quaterdecies: attribuzioni di funzioni e compiti a soggetti designati*

Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR (7 luglio 2021)

Parere 22/2024 su determinati obblighi derivanti dall'affidamento a responsabili del trattamento e sub-responsabili del trattamento (7 ottobre 2024)

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Il titolare del trattamento

Il titolare deve decidere *("must decide both purposes and means")* sia le finalità che i mezzi

I mezzi essenziali/vs i mezzi non essenziali

I "mezzi essenziali" sono tradizionalmente e intrinsecamente riservati al **titolare** e sono strettamente **collegati** ai dati trattati, alle basi giuridiche del trattamento e alle **finalità**
I "mezzi non essenziali" possono essere determinati pure dal **responsabile del trattamento**

*"**Non-essential means**" concern more **practical aspects** of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on*

Titolare sempre responsabile dell'attuazione di adeguate misure tecniche e organizzative

Nel contratto vanno indicate le misure

tenuto conto della natura, dell'ambito, del contesto, delle finalità del trattamento, nonché dei rischi

Il contitolare del trattamento

Due o più soggetti che determinano finalità e mezzi del trattamento

*Il trattamento non sarebbe possibile senza la **partecipazione delle parti in gioco***

Il **trattamento** di ciascuna delle parti è **inseparabile**, cioè **indissolubilmente legato**

La **partecipazione congiunta** deve includere («**needs**») la **determinazione degli scopi e dei mezzi**

Diversi titolari congiunti possono definire finalità e modalità del trattamento in misura diversa

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Il contitolare del trattamento
Una recente sentenza della Corte di giustizia*

Sent. 7 marzo 2024 nella causa C-604/22

la contitolarità, non presuppone che ciascuno dei contitolari abbia accesso ai dati personali

l'esistenza di una contitolarità non si traduce necessariamente in una responsabilità equivalente, per uno stesso trattamento di dati personali, dei diversi attori

I contitolari possono essere coinvolti in fasi diverse del trattamento e a diversi livelli quindi il grado di responsabilità di ciascuno di essi deve essere valutato tenendo conto di tutte le circostanze rilevanti del caso di specie

La partecipazione alla determinazione delle finalità e dei mezzi del trattamento può risultare sia da una decisione comune adottata da due o più soggetti che da decisioni convergenti

dette decisioni devono integrarsi, di modo che ciascuna di esse abbia un effetto concreto sulla determinazione delle finalità e dei mezzi del trattamento

* (cfr: sentenza del 10 luglio 2018, Jehovan todistajat, C 25/17, punti 66 e 69, nonché giurisprudenza ivi citata; Fashion ID GmbH & Co. KG Verbraucherzentrale NRW eV C-40/17)

L'accordo di contitolarità

I contitolari del trattamento **determinano** e **concordano** in modo trasparente le **rispettive responsabilità** per il rispetto degli obblighi previsti dal GDPR attraverso **l'accordo di contitolarità** (accordo interno a rilevanza esterna)

La determinazione delle responsabilità deve riguardare in particolare **l'esercizio dei diritti** degli interessati e gli **obblighi informativi**

Ciascun contitolare deve disporre di una **base giuridica** per il trattamento e i dati non possono essere **ulteriormente trattati** in modo incompatibile rispetto le finalità per le quali sono stati originariamente raccolti

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Il responsabile del trattamento

Nel Regolamento vi sono specifiche disposizioni che impongono obblighi direttamente ai responsabili del trattamento

- ✓ **designazione del rappresentante** (art. 27)
- ✓ **registro delle attività di trattamento** (art. 30)
- ✓ **cooperazione** con **l'Autorità** di controllo (art. 31)
- ✓ messa in atto di **misure tecniche e organizzative** idonee, per garantire un livello di sicurezza adeguato al rischio (art. 32)
- ✓ obbligo di **informare il titolare** del trattamento senza ingiustificato ritardo delle **violazioni di dati personali** (art. 33, par. 2)
- ✓ **designazione di un responsabile della protezione dei dati**, laddove previsto (art. 37)
- ✓ rispetto delle **condizioni per il trasferimento dei dati** verso un paese terzo o una organizzazione internazionale

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

- ✓ l'individuazione dei ruoli privacy è strettamente correlata ad una valutazione sostanziale e non formale dei trattamenti
- ✓ risulta difficile seguire e perseguire la stessa soluzione con una impostazione privacy aprioristica e preconfezionata cristallizzando i ruoli in via generale
- ✓ il ruolo di Titolare piuttosto che di Responsabile, in omaggio al principio di *accountability* deve essere attribuito in base a una valutazione fatta «*case by case*»

edpb European Data Protection Board

EDPB n. 7/2020
on the concept of controller and processor under the GDPR

- ✓ Sponsor e un'università cointitolari del trattamento
- ✓ Sponsor titolare e centro sperimentale responsabile del trattamento
- ✓ Sponsor e centro sperimentale titolari autonomi del trattamento

1) Ruolo delle Regioni quando mettono a disposizione dei diversi Enti del sistema sanitario regionale piattaforme/sistemi informativi

- ✓ la **valutazione** richiede una analisi «***case by case***» (principio di *accountability* e *privacy by design*);
- ✓ si potrebbero configurare degli scenari in cui la **Regione** è titolare del trattamento se **definisce** il **processo di identificazione** dell'assistito sulla piattaforma ma limitatamente a tali trattamenti;
- ✓ con riferimento alla **gestione tecnica** ed **informatica** della piattaforma, l'**ente del sistema sanitario regionale (es. ASL)** è **titolare** dei dati dei propri assistiti e alla Regione va attribuito il ruolo di **responsabile;**
- ✓ **condivisione delle politiche di sicurezza** che il titolare deve comunque accettare e valutare idonee a garantire l'integrità e la riservatezza dei dati dei propri assistiti gestiti attraverso la piattaforma/app ecc;
- ✓ il **Titolare** deve poter chiedere **ulteriori misure se necessarie** e il **Responsabile** deve implementarle.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

2) Ruolo delle società *in house* che sviluppano servizi di natura tecnica

Ferma la valutazione «***case by case***» che è necessario effettuare in omaggio al principio di *accountability*, nella maggior parte dei casi il ruolo delle ***società in house*** si configura quale **Responsabile** del trattamento

Provvedimento del 14 gennaio 2021 (doc. web n. 9542136)

Provvedimento del 1 dicembre 2022 (doc. web n. 9871846)

Provvedimento del 27 novembre 2024 (doc. web n. 10095810)

Numerosi precedenti del Garante

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Provvedimento del 14 gennaio 2021 (doc. web n. 9542136)

- ✓ l'istruttoria ha riguardato la fornitura del servizio di call center da parte di un soggetto esterno al titolare del trattamento;
- ✓ il Garante ha ribadito che le società che prestano servizi per conto del titolare devono essere designate responsabili del trattamento;
- ✓ il rapporto tra titolare e responsabile deve essere regolato da un contratto o da altro atto giuridico, stipulato per iscritto;
- ✓ il mancato ricorso da parte della Regione alla Società esterna quale responsabile del trattamento ha comportato un trattamento illecito di dati personali, in quanto sono state effettuate operazioni di trattamento dei dati raccolti nell'ambito del servizio ReCup di cui la Regione è titolare, in assenza di un idoneo presupposto di liceità.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Provvedimento del 1° dicembre 2022 (*doc. web n. 9871846*)

- ✓ l'istruttoria ha rigurdato **l'accesso non autorizzato ai dati personali** di cittadini di una Regione che avevano aderito alla campagna di vaccinazione attraverso **una applicazione web sviluppata dalla Società in house della Regione;**
- ✓ il Garante ha accertato che i trattamenti svolti dalla Società in house r**ientravano nel perimetro di titolarità della Regione**, in quanto afferenti a iniziative di sanità pubblica connesse all'espletamento della campagna vaccinale anti Covid-19 e che la Società era un responsabile del trattamento;
- ✓ ciò ha comportato la **violazione da parte della Regione** del principio di "**liceità, correttezza e trasparenza**" del trattamento, specie con riferimento alle informazioni fornite agli interessati che sono state contraddittorie in ordine a tali aspetti del trattamento;
- ✓ il Garante ha inoltre accertato la violazione del **principio di integrità e riservatezza, degli artt. 25, 32, 33 e 34 del Regolamento.**

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Provvedimenti del 27 novembre 2024 (*doc. web n. 10095810*)

- ✓ il Garante ha accertato che la violazione di dati personali oggetto di notifica di DB era stata provocata da un ***bug* di sicurezza** nel **sistema di autenticazione** del portale con cui si accedeva al FSE di una Regione

L'Autorità ha **sanzionato**:

- ✓ la **Regione** in quanto **titolare del Portale** (per la violazione dei principi di integrità e riservatezza e di protezione dei dati fin dalla progettazione e per impostazione predefinita);

- ✓ la **società *in house***, in qualità di responsabile dell'attività di **implementazione tecnica del FSE**, per non aver implementato misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, come previsto dall'atto di nomina a responsabile, (violazione dell'art. 32 RGPD);

- ✓ Il **sub-responsabile,** quale soggetto responsabile della progettazione e della realizzazione tecnica del sistema informatico impiegato per la gestione del fascicolo sanitario elettronico **per la violazione dell'art. 32 del RGPD** in quanto non ha implementato misure adeguate e per non averne regolarmente testato l'efficacia.

Decisione AEPD del 7 novembre 2024

- ✓ Marina Salud S.A., società per azioni spagnola, che gestisce i servizi sanitari per conto del Ministero della salute, **per mancata gestione dei sub responsabili;**
- ✓ affidamento di forniture IT a sub-responsabili senza averlo previamente comunicato al Titolare come previsto nel contratto ai sensi dell'art. 28 del GDPR;
- ✓ violazione valutata come grave, soprattutto considerando che i dati trattati riguardano quelli relativi alla salute;
- ✓ *data protection* non è solo un tema di sicurezza informatica, ma anche una questione di governance e compliance organizzativa.

3) I ruoli di protezione dei dati nell'ambito della aggregazioni funzionali territoriali tra medici di medicina generale/pediatri di libera scelta, farmacie, ecc

Le AFT (art. 8 decreto-legge 13 settembre 2012, n. 158 e Accordi Collettivi Nazioni, ACN)

- ✓ forme **organizzative mono-professionali** che condividono, in forma strutturata, obiettivi e percorsi assistenziali, strumenti di valutazione della qualità assistenziale ecc.;
- ✓ gli ACN disciplinano tra le altre cose, le condizioni, i requisiti e le modalità con cui le regioni provvedono alla dotazione strumentale e organizzativa;
- ✓ I medici che costituiscono la AFT sono **funzionalmente connessi** tra loro mediante una **struttura informatico-telematica di collegamento tra le schede sanitarie individuali degli assistiti** che consenta**, nel rispetto della normativa sulla privacy e della sicurezza nella gestione dei dati**, l'accesso di ogni medico della AFT ad informazioni cliniche degli assistiti degli altri medici operanti nella medesima AFT per una efficace presa in carico e garanzia di continuità delle cure.

Vi possono essere diversi modelli sul territorio

- ✓ l'ACN non affronta gli aspetti di protezione dei dati personali, tra cui quello dei ruoli e del presupposto di liceità che consentirebbe ai medici di trattare i dati dei pazienti in condivisione tra di loro (**nella prossima contrattazione tali aspetti potrebbero essere indirizzati**);
- ✓ l'attribuzione dei ruoli deve essere fatta sulla base del modello di AFT che è previsto a livello territoriale tenendo anche in considerazioni i mezzi del trattamento e il rapporto fiduciario medico - paziente;
- ✓ in concreto si potrebbe ipotizzare un rapporto di contitolarità tra i diversi medici, di titolarità autonoma, con i conseguenti impatti in termini di obblighi informativi e di esercizio dei diritti;
- ✓ resta fermo il principio della pertinenza delle informazioni cui posso avere accesso necessarie per l'espletamento delle proprie funzioni istituzionali dei diversi soggetti.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

App mediche

Compendio sul trattamento dei dati personali attraverso piattaforme volte a mettere in contatto i pazienti con i professionisti sanitari accessibili via web e app - marzo 2024
doc. web n. 9997624

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

App e piattaforme mediche

- 3 macro tipologie di trattamenti
- Finalità e basi giuridiche
- Coordinamento con altri strumenti normativi (FSE, dossier sanitario, referti on line)
- Ruoli privacy
- VIP/Misure di sicurezza
- Trasparenza

GPDP
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

MARZO 2024

COMPENDIO

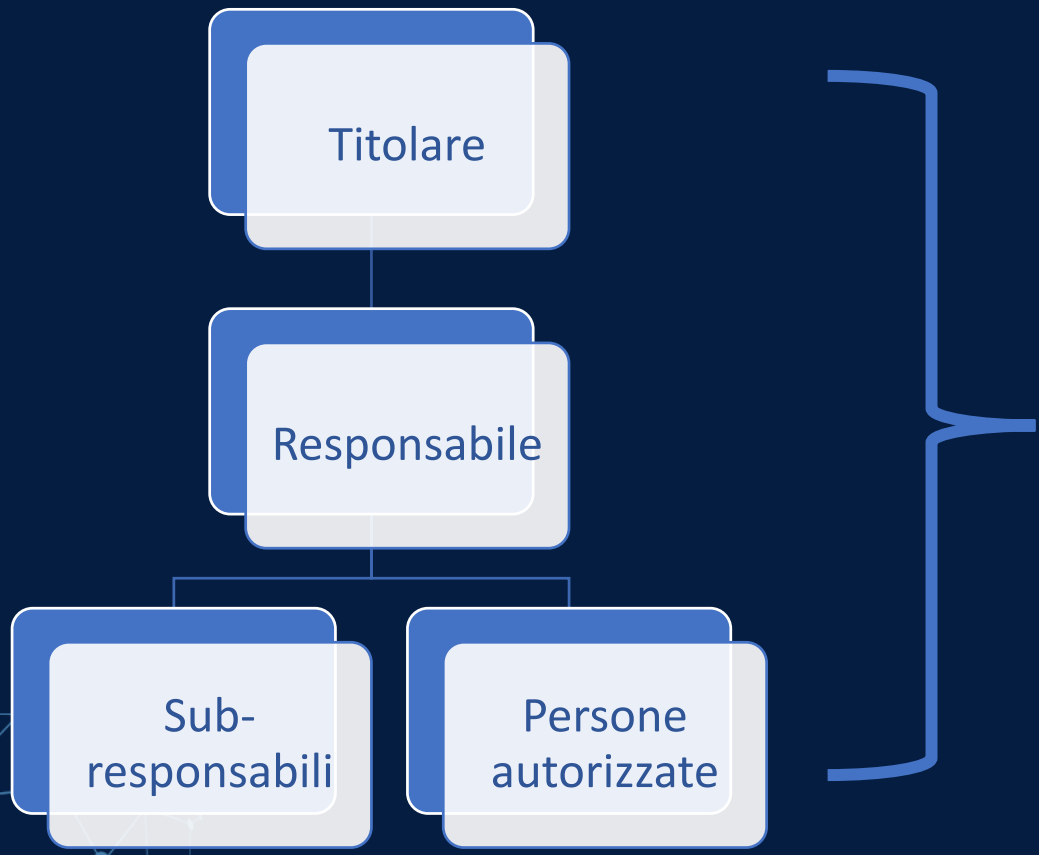
sul trattamento dei dati personali effettuato attraverso piattaforme volte a mettere in contatto i pazienti con i professionisti sanitari accessibili via web e app

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

I RUOLI



GOVERNANCE DEI DATI

I ruoli vanno individuati avendo una visione complessiva delle operazioni di trattamento che tenga conto delle diverse finalità per le quali i trattamenti sono svolti e dunque delle diverse basi giuridiche sulle quali essi si fondono

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

TELEMEDICINA METODOLOGIE PREDITTIVE

Silvia Melchionna
Dipartimento sanità e ricerca

11 giugno 2025

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

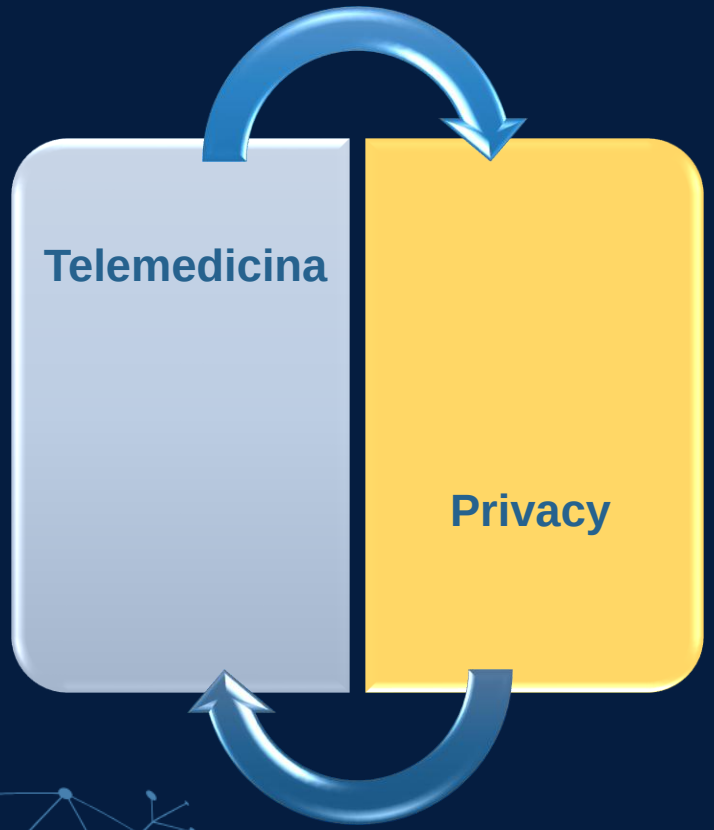
TELEMEDICINA

Assetto Privacy delle piattaforme regionali e basi giuridiche per trattamenti specifici. Necessità di confrontarci sui ruoli privacy dei diversi soggetti coinvolti. Legittimità e base giuridica della registrazione delle televisita e successiva archiviazione

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca



GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Servizi di telemedicina

Sistemi centrali di telemedicina

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

SENZA CONSENSO

per fini di cura*

(FAQ Covid)

INFORMATIVA

VALUTAZIONE D'IMPATTO

SERVIZI DI TELEMEDICINA

***a eccezione dei trattamenti non strettamente necessari**

VALUTAZIONE D'IMPATTO PRIVACY

OBBLIGATORIA

USO TECNOLOGIE INNOVATIVE

Registrazione televisita da parte del titolare

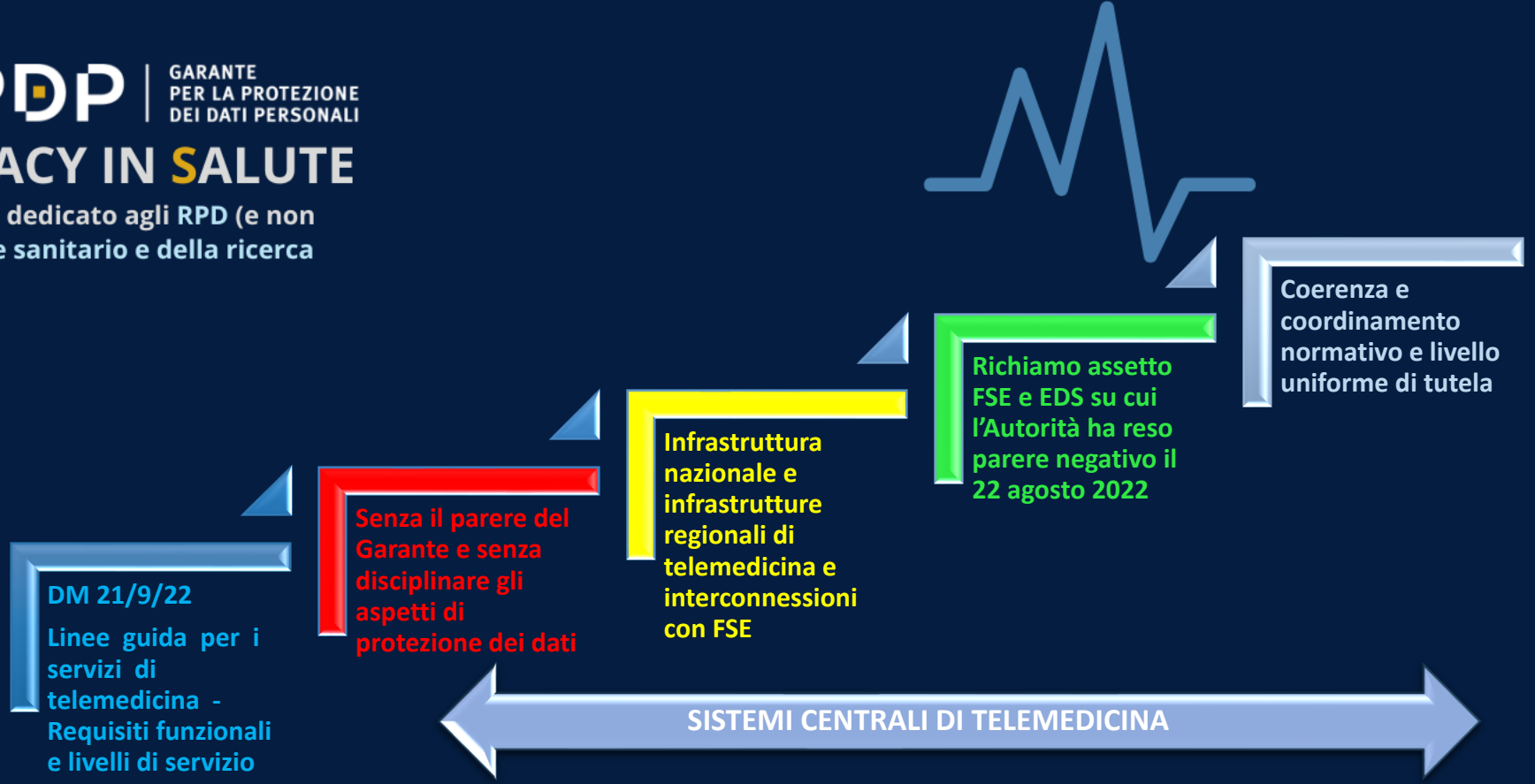
- Registrazione è un trattamento
- Base giuridica dipende da finalità
- Finalità di cura senza consenso solo se strettamente necessario
- Informativa
- Soggetti terzi
- Periodo di conservazione

Codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica
14 gennaio 2021 - *doc. web n. 9535354*

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca



PARERE DEL GARANTE DELL'8 GIUGNO 2023 SUL FSE 2.0

PIATTAFORMA NAZIONALE DI TELEMEDICINA

- Art. 12, c. 15 undecies, lett. g) e h) dl n. 179/2012
- Agenas gestisce la PNT
- SCHEMA DECRETO PNT
- Parere 16/1/25, doc. web n. 10105743
- Parere ACN 11/3/25 con osservazioni su profili di cybersicurezza
- Decreto non ancora adottato

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

PIATTAFORMA NAZIONALE DI TELEMEDICINA

Schema di decreto su cui ha espresso il parere il Garante

SERVIZI MINIMI DI TELEMEDICINA
(televisita, teleconsulto, telemonitoraggio, teleassistenza)

EROGATI TRAMITE IRT

Regioni/P.A. possono erogare prestazioni di telemedicina con modalità diverse ma con infrastrutture certificate da Agenas

PNT

IRT E INT

L'INT offre alle IRT servizi abilitanti a supporto del processo di cura e nell'erogazione delle prestazioni di telemedicina creando un livello di interoperabilità che garantisce standard comuni

PNT/FSE

CONFERIMENTO DATI FSE e ACCESSO A FSE

Tramite IRT

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Schema di decreto su cui ha espresso il parere il Garante

Assistito → **Informativa da Regioni/ Province autonome** → **Accede alla IRT tramite portale dedicato**

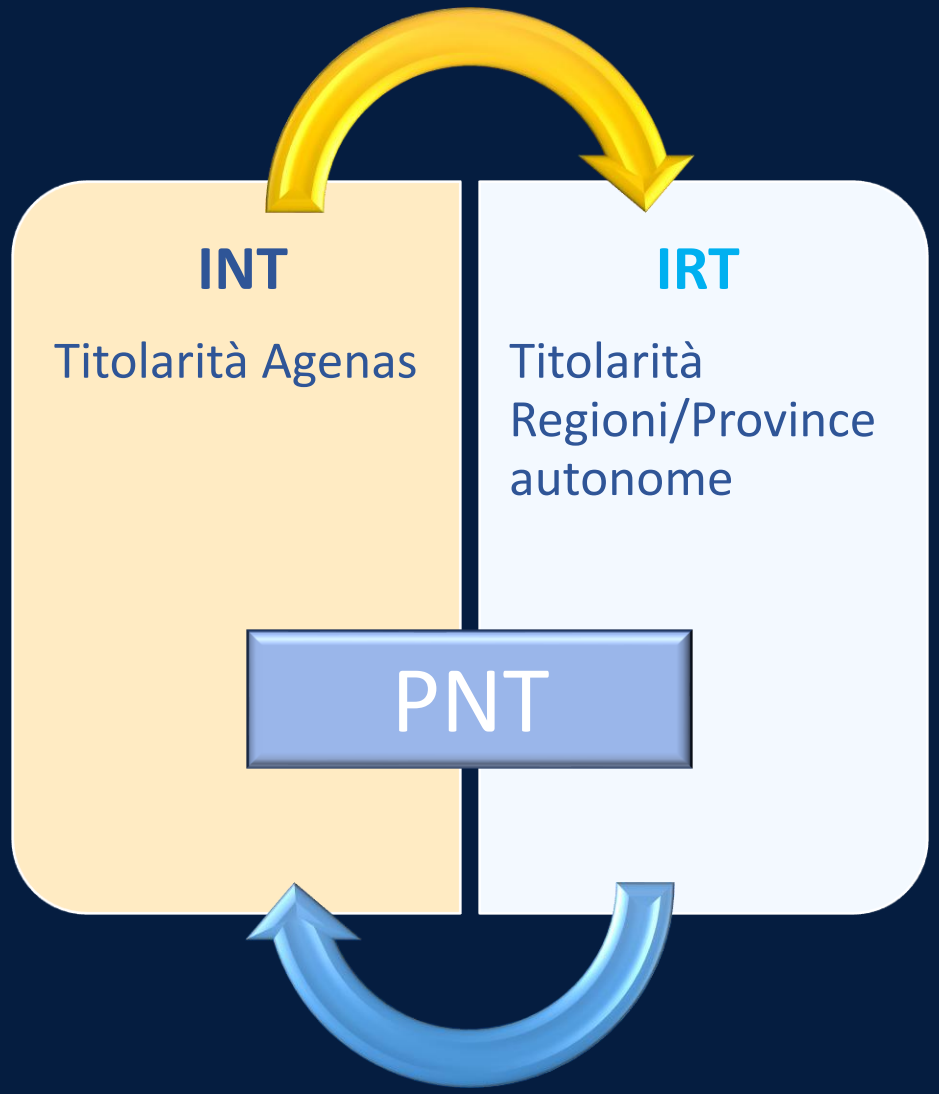
Personale curante → **Accede a IRT** → **Titolari dei trattamenti che effettuano attraverso i servizi offerti da IRT**

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Schema di decreto su cui ha espresso il parere il Garante



GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Schema di decreto su cui ha espresso il parere il Garante

PIATTAFORMA NAZIONALE DI TELEMEDICINA

REVISIONE LINEE GUIDA 2022

I trattamenti effettuati dalla PNT per finalità diverse da quelle di diagnosi, cura e riabilitazione descritti nelle richiamate Linee Guida sono sospesi

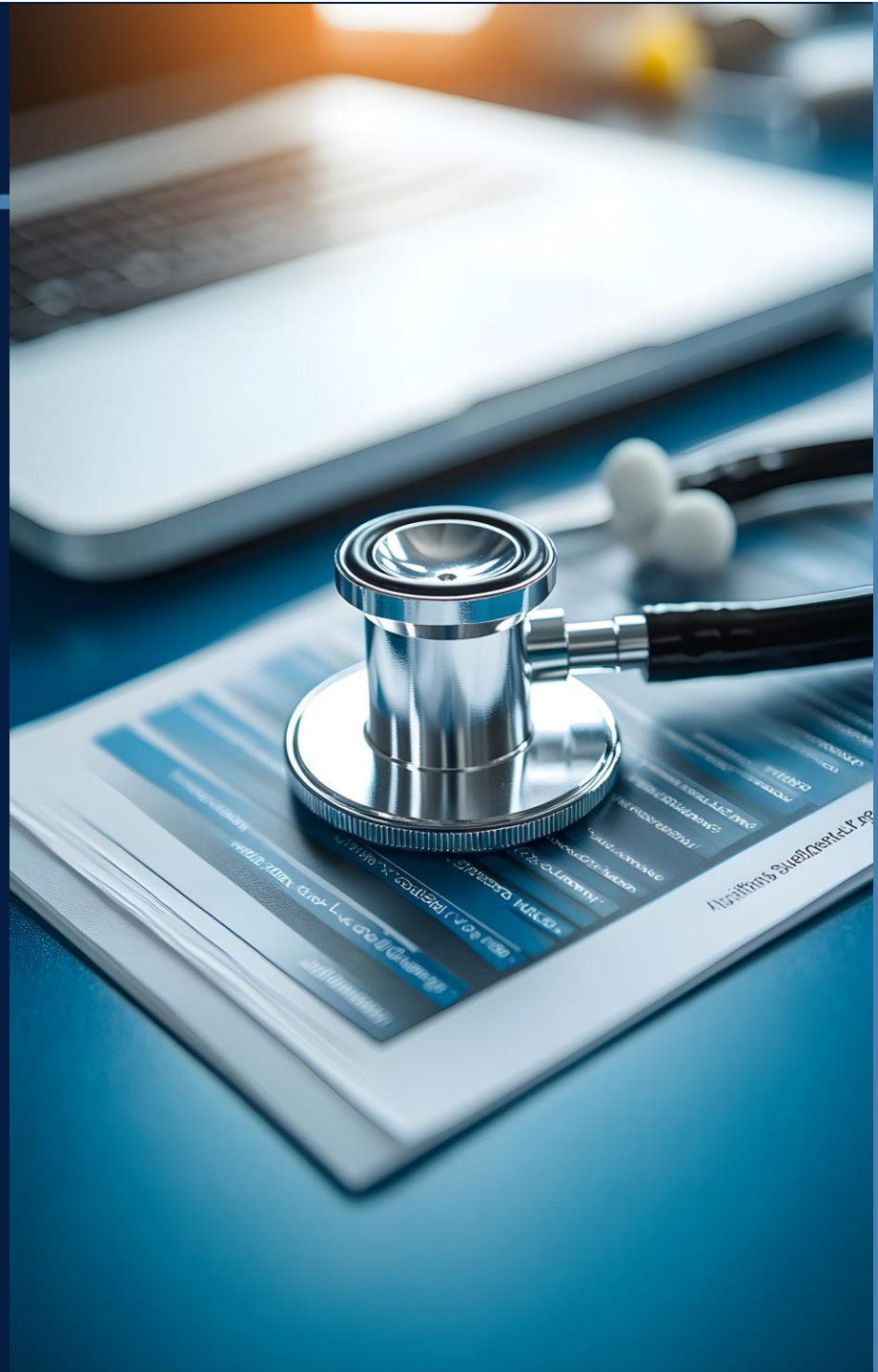
fino all'aggiornamento delle medesime con decreto da adottare previo parere del Garante

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

METODOLOGIE PREDITTIVE



GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Nell'ambito di iniziative volte allo sviluppo di metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione residente e/o del singolo paziente nell'ambito di un'Asl e/o di c.d. medicina d'iniziativa, possa ritenersi base giuridica adeguata dei necessari trattamenti di dati, anche appartenenti alle c.d. categorie particolari, il solo consenso dell'interessato, ovvero se possano essere richiamate allo scopo previsioni normative, ovvero ancora se, allo stato, tali finalità debbano ritenersi precluse.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

DATO SANITARIO

PROFILAZIONE

CLASSI DI RISCHIO

STRATIFICAZIONE

INTERVENTI DI CURA E DI GOVERNO

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

- profilazione su dati sanitari è un trattamento automatizzato per cui necessita di una espressa previsione normativa conforme al GDPR

Parere Consiglio di Stato 5 marzo 2020

doc. web n. 9304455

Art. 7 D.L. 34/2020

- metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione
- decreto attuativo

- pareri Provincia Trento (8/5/202- doc. web 9344635; 1/10/2020 – doc. web n. 9469372)
- provvedimento Ausl toscana sud est (17/12/2020- doc. web n. 9529527)

Iniziative regionali

ART. 7, D.L. N. 34/2020

Il MdS, nell'ambito dei fini istituzionali (coordinamento, programmazione, monitoraggio tecnico sanitario di rilievo nazionale), per lo sviluppo di metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione, con le modalità di cui al d.m. n. 262/2016 (decreto interconnessioni), può:

- ✓ trattare dati sulla salute, raccolti nei sistemi informativi del SSN;
- ✓ interconnettere i sistemi informativi su base individuale del SSN, ivi incluso il FSE, con i sistemi informativi gestiti da altre amministrazioni pubbliche che raccolgono dati non relativi alla salute.

Con decreto (parere del Garante) sono individuati: i dati che possono essere trattati, le operazioni eseguibili, le modalità di acquisizione dei dati dai sistemi informativi dei soggetti che li detengono e le misure appropriate e specifiche per tutelare i diritti degli interessati, nonché i tempi di conservazione dei dati trattati.

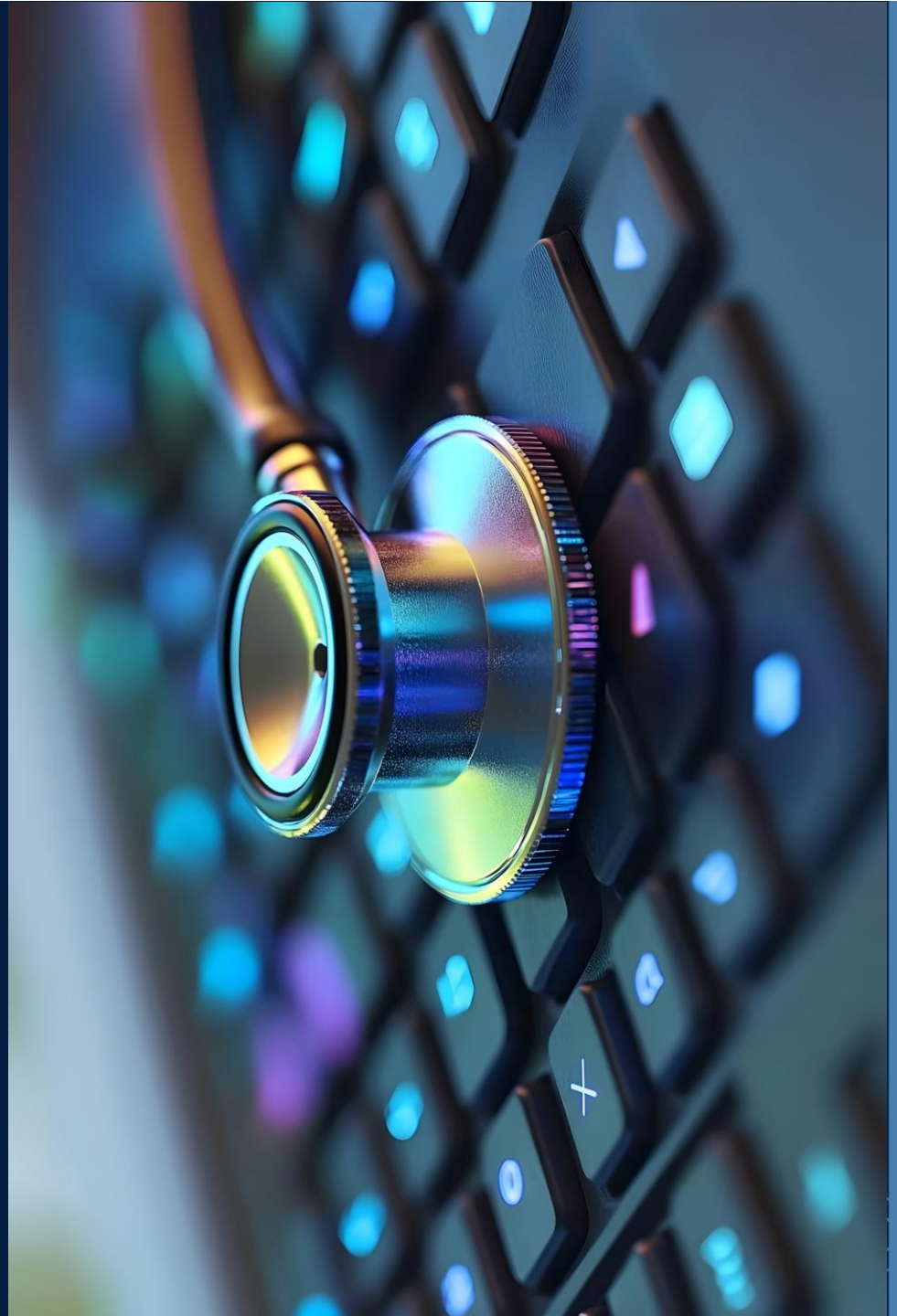
Nelle more del decreto, il Ministero avvia le attività relative alla classificazione delle patologie croniche presenti nella popolazione italiana, limitatamente alla costruzione di modelli analitici prodromici alla realizzazione del modello predittivo del fabbisogno di salute della popolazione, garantendo che gli interessati non siano direttamente identificabili.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

ART. 7 D.L. 34/2020



PROVVEDIMENTI DI AMMONIMENTO - 24 FEBBRAIO 2022

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

D.M. 77 DEL 2022

DEFINIZIONE DEI MODELLI E STANDARD PER LO SVILUPPO DELL'ASSISTENZA TERRITORIALE NEL SERVIZIO SANITARIO NAZIONALE

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Elaborazione dati

Profilo sanitario di rischio

Fini di cura

Trattamento autonomo non strettamente necessario

Consenso interessato + VIP

RISPETTO DISCIPLINA DI SETTORE

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Accesso alla cartella clinica ai sensi dell'art. 15 del RGPD. Chiarimenti dell'Autorità attraverso FAQ a seguito della sentenza CGUE-307/22

Giovanna Iadeluca
Dipartimento sanità e ricerca
11 giugno 2025

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

FAQ rintracciabili nel sito web istituzionale, nella pagina:

https://www.gpdp.it/temi/sanita-e-ricerca-scientifica/cartelle-cliniche

oggetto della NewsLetter del 23 dicembre 2024, alla pagina:

https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10086101

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

RECLAMI ex art. 77 del Regolamento per il mancato rilascio gratuito, da pardi talune strutture ospedaliere, della prima copia documentale della propria cartte ella clinica

Nei reclami si invocava la sentenza CGUE-307/2022

CGUE-307/2022 del 26 ottobre 2023

rinvio pregiudiziale operato dalla Corte federale di giustizia tedesca

Comunicato stampa della Corte di Giustizia UE n. 161/23 del 26 ottobre 2023:

“**Protezione dei dati personali: il paziente ha il diritto di ottenere gratuitamente una prima copia della sua cartella medica**”.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Prima copia gratuita della propria cartella medica

- COPIA DEI DATI
- COPIA DEI DOCUMENTI

GPDP | PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

CGUE C-307/22

3 QUESTIONI PREGIUIDIZIALI

TERZA QUESTIONE: il giudice del rinvio aveva chiesto alla Corte se, nell'ambito di un **rapporto medico-paziente**, la locuzione "*copia dei dati personali oggetto di trattamento*" di cui all'articolo 15, paragrafo 3, prima frase, dovesse essere nel senso che conferisce all'interessato un diritto generale di ottenere una copia integrale dei documenti inclusi nella sua cartella medica e che contengono i suoi dati personali o soltanto una copia di detti dati in quanto tali.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

Sulla terza questione la CGUE ha statuito che:

«L'articolo 15, paragrafo 3, prima frase, del Regolamento 2016/679 deve essere interpretato nel senso che nell'ambito di un rapporto medico/paziente, il diritto di ottenere una copia dei dati personali oggetto di trattamento implica che sia consegnata all'interessato una riproduzione fedele e intelligibile dell'insieme di tali dati.

Tale diritto presuppone quello di ottenere la copia integrale dei documenti contenuti nella sua cartella medica che contengano, tra l'altro, detti dati, qualora la fornitura di una siffatta copia sia necessaria per consentire all'interessato di verificarne

Per quanto riguarda i dati relativi alla salute dell'interessato, tale diritto include in ogni caso quello di ottenere una copia dei dati della sua cartella medica contenente informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati al medesimo».

- *esattezza*
- *completezza*
- *intelligibilità*

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

ART. 15 DEL REGOLAMENTO

Accesso ai dati personali

L'interessato ha diritto di ottenere dal titolare del trattamento:

1) *la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano*

2) l'accesso alle informazioni di cui ai paragrafi 1 (lettere da a) ad h)) e 2 dell'art. 15 del Regolamento

3) copia dei dati personali.

La prima copia di tali dati è gratuita

(art. 15, par. 3 e art. 12, par. 5 del Regolamento)

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

CARTELLA CLINICA

- d.P.R. 1631 del 30 settembre 1938
- d.P.R. 27 marzo 1969, n. 128, artt. 5 e 7
- D.M. Sanità del 5 agosto 1977, art. 24
- D.P.C.M. del 27 giugno 1986, art. 35
- D.M. del 28 dicembre 1991
- D.M. n. 380 del 27 ottobre 2000
- Circolare Ministero Sanità 19 dicembre 1986, n. 900
- Linee guida Ministero Salute 17 giugno 1992
- Codice deontologia medica art. 26
- D.lgs. 196/2003 – art. 92

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

DECRETO LEGISLATIVO 30 giugno 2003, n.196
recante il "Codice in materia di protezione dei dati personali»
Art. 92 (Cartelle cliniche)

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

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

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

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

CARTELLA CLINICA

strutture pubbliche e private convenzionate

Atto amministrativo pubblico - disciplina dell'art. 2699 c.c. - piena prova fino a querela di falso (ex multiis: Cass. pen, Sez. V, sent. 19557/2010; ex multis: Cass. n. 37314 del 29.05.2013; Cass. pen. Sez. V, sent. 9393/2019).

D.P.R. 128/1969

CARTELLA CLINICA

Case di cura private

Le cartelle cliniche delle case di cura private devono essere annotate come disposto dall'art. 24 del D.M. Sanità del 5 agosto 1977

CARTELLA/SCHEDA

del medico libero-professionista privato

Artt. 25 e 26 codice deontologico

Art. 25
Documentazione sanitaria

Art. 26
Cartella clinica

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

FAQ

Cosa si ottiene presentando istanza di accesso alla propria cartella clinica ai sensi dell'art. 15 del RGPD: copia dei dati personali o copia della documentazione?

L'interessato può accedere, ai sensi dell'art. 15 del RGPD, alla propria cartella clinica ottenendo copia dei dati personali oggetto di trattamento (art. 15, par. 3, del RGPD). Il titolare fornisce all'interessato copia integrale dei documenti contenenti tali dati, qualora lo ritenga necessario per garantire esattezza, completezza e intelligibilità delle informazioni richieste (sentenza CGUE 307-22 del 26 ottobre 2023).

Con la richiesta di accesso alla cartella clinica, presentata ai sensi dell'art. 15 del RGPD, l'interessato può pretendere di ottenere a titolo gratuito la prima copia di tutta la documentazione contenuta in tale cartella?

No. Attraverso la richiesta di accesso alla cartella clinica ai sensi dell'art. 15 RGPD viene fornita a titolo gratuito la prima copia dei dati personali (art. 12, par. 5 e art. 15, par. 3, del RGPD) che, come evidenziato nella faq precedente, non necessariamente consiste in una copia dei documenti contenuti in tale cartella.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LA PRIVACY IN SALUTE

Ciclo di incontri dedicato agli RPD (e non solo) del settore sanitario e della ricerca

FAQ

Chi valuta la necessità di fornire copia integrale dei documenti contenuti nella cartella clinica a fronte di una richiesta di accesso ai dati di cui all'art. 15 del Regolamento?

Il titolare del trattamento. (cfr. in tal senso il documento del Comitato europeo per la protezione dei dati (EDPB) "Linee guida 1/2022 sui diritti degli interessati - Diritto di accesso" - versione 2.1 del 28 marzo 2023 - punto 152, rintracciabili all'indirizzo web: https://www.edpb.europa.eu/system/files/2024-04/edpb_guidelines_202201_data_subject_rights_access_v2_it.pdf).

A fronte di una generica istanza di accesso alla cartella clinica, non presentata formalmente ai sensi dell'art. 15 del RGPD, come deve comportarsi il titolare del trattamento?

Il Regolamento non prevede requisiti formali per la presentazione di richieste di accesso ai dati personali. In caso di dubbi, si raccomanda al titolare del trattamento una certa indulgenza nei confronti dei richiedenti, spesso non a conoscenza delle complesse disposizioni del RGPD e di chiedere all'interessato che presenta la richiesta di accesso di specificare l'oggetto della richiesta stessa (cfr. Linee guida sopracitate, punto n. 50)