Aspetti legali: privacy e trattamento dati

Dott.ssa Alessandra Migliore
Responsabile Protezione Dati
A.O.U. Città della Salute della Scienza di Torino

Il trattamento dati in ambito sanitario

- Il trattamento dei **dati particolari** nella sanità

Contesto molto delicato in ragione della natura dei dati

→ Dati *ultrasensibili*

Il trattamento dati in ambito sanitario

- Gli organismi sanitari devono poter **disporre e trattare** tutti i dati necessari e tutte le informazioni che riguardano le relazioni che intercorrono tra l'utente, il medico ed i servizi.
- L'utilizzo di tali dati non deve sconfinare nell'abuso.

Il trattamento dati in ambito sanitario

- Nuove tecnologie:
  - *La dematerializzazione;*
  - *Le cartelle cliniche digitali;*
  - *I dispositivi medici mobile;*
  - *I referti online;*
  - *Il dossier e il fascicolo sanitario elettronico*.

Il trattamento dati in ambito sanitario

- Primi riferimenti normativi:
  - ***Legge 675/1996.***
  - ***Decreto Legislativo 196/2003,*** poi modificato dal ***Decreto Legislativo 101/2018.***

- Successivamente:
  - ***Regolamento (UE) 2016/679 (GDPR)***

I RUOLI

Ruoli:
I Soggetti del Trattamento

- Interessato

Ruolo passivo

- Titolare
- Contitolari
- Responsabile
- Subresponsabili
- Autorizzati
- Rappresentante

Ruoli attivi

- DPO

Ruolo misto di controllo/ consulenza

TIPOLOGIE DI DATI

Dati relativi alla salute

Articolo 4 GDPR:

I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Dati relativi alla salute

*Il **Considerando 35 del GDPR** specifica che vengono compresi:*

- *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;*
- *Informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria;*
- *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;*
- *Qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica ecc.*

Il dato anonimo

Considerando 26:

“informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l’identificazione dell’interessato.”

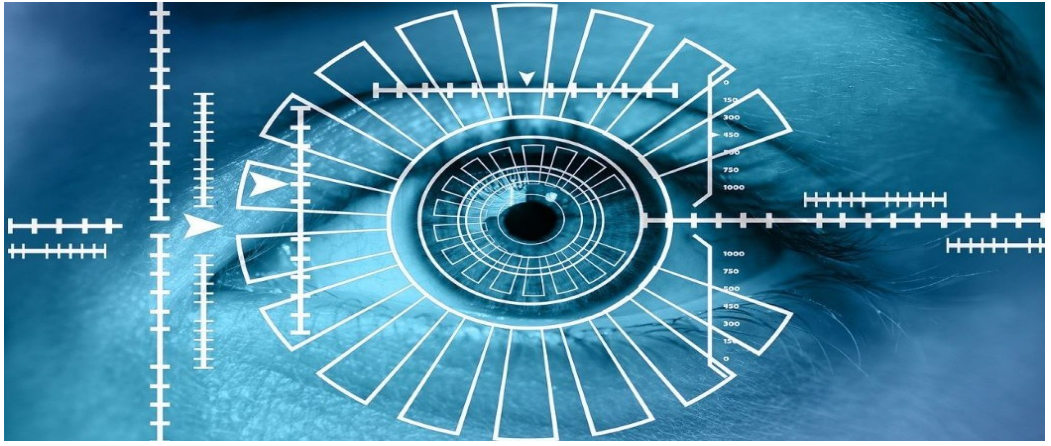
La pseudonimizzazione non è la stessa cosa dell’anonimizzazione!

- l’uso di “informazioni aggiuntive” può portare all’identificazione degli individui, motivo per cui i dati personali pseudonimi sono ancora dati personali.

- I dati anonimi non possono essere associati a individui specifici. Una volta che i dati sono veramente anonimi e gli individui non sono più identificabili, i dati non rientrano nell’ambito del GDPR.

Dati Biometrici

Sono ***dati biometrici***: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.



Dati Particolari

Articolo 9 GDPR:

Trattamento di categorie particolari di dati personali

- *1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*

- Il divieto **non si applica** in alcuni casi, come ad esempio:
- Consenso esplicito dell'interessato;
- Assolvere gli obblighi in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- Tutelare un interesse vitale dell'interessato.

TRATTAMENTO DATI

Trattamenti di dati personali

Esempi:

- Raccolta.
- Registrazione.
- Organizzazione.
- Strutturazione.
- Conservazione.
- adattamento o la modifica.
- Estrazione.
- Consultazione.
- Uso.
- Comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione.
- Raffronto o interconnessione.
- Limitazione.
- Cancellazione.
- Distruzione.

Provvedimento del Garante 7 marzo 2019

- Il trattamento dei dati sulla salute è consentito in presenza di alcuni requisiti specifici (*art.9 GDPR*)
- Possibilità per gli stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni.
- Il *d.lgs n.101/2018* ha previsto che il Garante completi l'individuazione dei presupposti di liceità dei trattamenti, adottando specifiche misure di garanzia e promuovendo l'adozione di regole deontologiche.

Trattamento di dati relativi alla salute

Eccezioni che rendono lecito il trattamento:

- Motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
- Motivi di interesse pubblico nel settore della sanità pubblica;
- Finalità di cura;

Non è richiesto il consenso

Trattamento di dati relativi alla salute

- App mediche;
- Trattamenti preordinati alla fidelizzazione della clientela;
- Trattamenti in ambito sanitario da persone giuridiche private per finalità promozionali o commerciali;
- Trattamenti in ambito sanitario da professionisti sanitario per finalità commerciali o elettorali;
- Fascicolo Sanitario Elettronico.

È richiesto il consenso

Trattamento di dati relativi alla salute

Nuove tecnologie:

- *La dematerializzazione;*
- *Le cartelle cliniche digitali;*
- *I dispositivi medici mobile;*
- *I referti online;*
- *Il dossier e il fascicolo sanitario elettronico*.

Rischi → **Data Breach**

DATA BREACH E REGISTRO DEI TRATTAMENTI

Data Breach

Art.33 GDPR

Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita , la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

- Nel caso in cui la violazione dati personali presenti un rischio per i diritti e le libertà delle persone fisiche:
- Notifica al Garante senza ingiustificato ritardo e, ove possibile, entro ***72 ore*** dal momento in cui ne è venuto a conoscenza;
- In caso di rischio elevato: comunicazione all'interessato *Art. 34* del GDPR.

Data Breach

- Provv. 4/4/2013, n.161 “Comunicazioni elettroniche” comunicazione al Garante entro 24h dalla conoscenza della violazione in forma sommaria ed entro 3 gg. In forma dettagliata.
- Provv. 12/11/2014, n.513 “Biometria” entro **24h** dalla conoscenza della violazione.
- Provv. 4/6/2015, n.331 “Dossier sanitario Elettronico” entro 48 h dalla conoscenza della violazione.
- Provv. 2/7/2015, n.293 “Pubblica Amministrazione” entro 48h dalla conoscenza della violazione.

Violazione dei Dati

- A partire dal 25 maggio 2018, tutti i Titolari dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro ***72 ore*** e comunque “senza ingiustificato ritardo”, se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.
- Superate le ***72 ore*** il Titolare deve motivare il ritardo.

Notifica di Data Breach

- Natura della violazione (accidentale o illecita);
- Numero e categorie di interessati;
- Numero e categorie di registrazioni dei dati personali;
- Contatti interni (DPO o altro);
- Stima delle conseguenze;
- Misure adottate o adottande.

Rischi per gli interessati

- Perdita del controllo dei dati personali o limitazione dei diritti;
- Discriminazione;
- Furto o usurpazione d'identità;
- Perdite finanziarie;
- Decifratura non autorizzata della pseudonimizzazione;
- Pregiudizio alla reputazione;
- Perdita di riservatezza dei dati personali protetti da segreto professionale;
- Qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Rischio elevato

- Se la probabilità di tale rischio è elevata, gli interessati dovranno essere informati della violazione, ***“senza ingiustificato ritardo”***.
- L'Autorità Garante può valutare la necessità di procedere alla comunicazione agli interessati richiedendo che il Titolare provveda.

Registro dei trattamenti

Art.30 GDPR

Tutti i Titolari e i Responsabili di trattamento devono tenere un registro delle operazioni di trattamento.

Strumento fondamentale per:

- eventuale supervisione del Garante;
- disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'azienda.

Requisito registro:

- forma scritta (anche elettronica);
- deve essere sempre aggiornato.

Registro dei trattamenti

Quali informazioni contiene?

- Nome e dati di contatto del titolare, del contitolare ove previsto, del dpo;
- Finalità del trattamento;
- Liceità del trattamento;
- Categorie degli interessati;
- Categorie dei dati;
- Categorie dei destinatari;
- Ove applicabile i trasferimenti verso un paese terzo o un’organizzazione internazionale;
- Termini di cancellazione;
- Descrizione delle misure di sicurezza tecniche ed organizzative.

Grazie dell'attenzione!