Prossimità e organizzazione delle cure: la medicina generale di domani tra demografia e cronicità

PRIVACY E MEDICINA GENERALE AD UN ANNO DALL'ENTRATA IN VIGORE DEL GDPR

Avv. Michele Langiulli

76° CONGRESSO NAZIONALE | 7-12 ottobre 2019 | Tanka Village - Villasimius (CA)

FIMMG Federazione Italiana Medici di Famiglia

SIMG Società Scientifica dei Medici

PRIVACY E MEDICINA GENERALE AD UN ANNO DALL'ENTRATA IN VIGORE DEL GDPR

I nuovi adempimenti: il registro delle attività di trattamento e la valutazione di impatto sulla protezione dei dati

Regole e principi generali

Approccio *risk based* e responsabilizzazione

Il regolamento ha il suo fulcro sulla responsabilizzazione del titolare e dei responsabili del trattamento (**accountability** vuol dire "dover rendere conto del proprio operato"), che si deve concretizzare nell'adozione di misure adeguate e concrete (e non meramente formali) e nella capacità di dimostrare in ogni momento non solo l'adozione ma anche l'efficacia di tali misure. Non basta più l'approccio formalistico ("ho il consenso e tratto il dato"), ma è necessario attuare misure di tutela e garanzia, con un approccio del tutto nuovo che **demanda ai titolari il compito di decidere autonomamente le modalità e i limiti del trattamento dei dati** alla luce dei criteri specifici indicati nel Regolamento:

- principio «privacy by design», in base al quale ogni trattamento dovrà essere progettato fin dall'inizio in modo da tutelare la privacy degli utenti, deve essere previsto e configurato cioè, fin dall'inizio, prevedendo le misure per tutelare i diritti degli interessati;

- rischio del trattamento, inteso come valutazione dell'impatto negativo sulle libertà e i diritti degli interessati.

Iter Logico – Giuridico del GDPR:

1) Cosa e come Tratto?

- le **operazioni svolte** sui dati (es. raccolta, registrazione, conservazione, ecc..),
- **tipologie** di dati trattati e finalità del trattamento,
- **cosa uso per trattarli** e dove (strumenti utilizzati e loro ubicazione),
- categorie di **interessati** (dipendenti, clienti, fornitori, pazienti ecc..),
- **destinatari** dei dati (interni e/o esterni, comunicazioni e/o trasferimenti),

Iter Logico – Giuridico del GDPR:

2) A quali rischi sono esposti i dati che tratto?

I parametri di cui tenere conto secondo l'art. 32 del GDPR sono:

- **riservatezza del dato,**
- **disponibilità del dato,**
- **integrità del dato.**

I valori di probabilità di verificarsi della minaccia sono:

- **Basso**: è improbabile che la minaccia si materializzi
- **Medio**: c'è una ragionevole possibilità che la minaccia si materializzi
- **Alto**: la minaccia potrebbe materializzarsi

I livelli di impatto sugli interessati possono essere:

basso: quando gli interessati andranno incontro a **disagi contenuti che supereranno senza problemi; medio**: quando gli interessati possono **avere significativi disagi che saranno in grado di superare nostante alcune difficoltà** (costi, stress, mancanza di comprensione ecc...)**; alto**: quando potranno esserci **conseguenze significative** che gli interessati **dovrebbero riuscire a superare anche se con gravi difficoltà** (liste nere di istituti finanziari, perdita di lavoro, danni alla proprietà, citazioni in giudizio, ecc...)**; molto alto**: quando gli interessati potranno subire **conseguenze significative o irreversibili che non saranno in grado di superare** (incapacità di lavorare, disturbi psicologici o fisici a lungo termine)

Iter Logico – Giuridico del GDPR:

3) Quali misure devo adottare?

Le minacce da valutare si possono valutare in quattro macro-aree :

- Risorse di rete e tecniche
- Processi e procedure
- Parti e persone coinvolte
- Settore e scala del trattamento

Il caso del MMG

Il registro dei trattamenti

L’obbligo di tenere il **registro dei trattamenti** è previsto dall'articolo 30 del Regolamento ed è a carico del titolare e, se nominato, del responsabile del trattamento.

La corretta tenuta del registro costituisce uno dei principali elementi di accountability del titolare, in quanto è utile per una completa ricognizione e valutazione dei trattamenti svolti. È anche strumento essenziale dell’analisi del rischio e di una corretta pianificazione dei trattamenti.

Il registro, che è un documento interno, deve essere tenuto in **forma scritta, anche in formato elettronico**, e va esibito all’autorità di controllo (Garante) in caso di verifiche. Ovviamente il registro deve essere costantemente aggiornato. Il registro deve anche recare "in maniera verificabile" sia la **data della sua prima istituzione** o creazione sia la **data dell’ultimo aggiornamento**.

Art. 30 Registri delle attività di trattamento

1. Ogni **titolare** del trattamento e, ove applicabile, il suo rappresentante tengono **un registro delle attività di trattamento svolte sotto la propria responsabilità**. Tale registro contiene tutte le seguenti informazioni:
   a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
   b) le finalità del trattamento;
   c) una descrizione delle categorie di interessati e delle categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
   e) …….. (trasferimenti);
   f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
2. Ogni **responsabile del trattamento** e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
   a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
   b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
   c) ……..;
   d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo (Garante).
5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Trattamento:	Descrizione:	Finalita':	Categorie:	Dati personali:	Destinatari:	Conclusione:
Acquisti	Il trattamento ha per oggetto le attivita' di ricerca e selezione dei fornitori per stipula dei contratti di fornitura di beni e/o servizi necessari alla gestione dello studio medico.	Attivita' di acquisto di beni o servizi (GDPR)	Fornitori	Coordinate bancarie Professione dichiarata Attivita' economiche, commerciali, finanziarie, assicurative Codice fiscale ed altri numeri di identificazione personale Nominativo, indirizzo o altri elementi di identificazione personale Dati di contatto (numero di telefono, e-mail, ecc.)	Consulenti e liberi professionisti in forma singola o associata Banche e istituti di credito	10 anni a decorrere dalla data di cessazione del contratto (prescrizione ordinaria in materia contrattuale) Data di inizio del trattamento: 22-05-2018
Assistenza pazienti	Il trattamento ha per oggetto l'attivita' di assistenza medica ai pazienti. Il trattamento comprende la registrazione anagrafica dei pazienti, la gestione delle relative cartelle cliniche, la gestione/archiviazione e trasmissione a terze parti delle prescrizioni o di altri dati sanitari e la gestione delle comunicazioni ai pazienti tramite i canali di contatto disponibili (corrispondenza ordinaria, e-mail, telefono).	Gestione del rapporto di cura con i pazienti (ACN di riferimento)	Pazienti e loro familiari	Sesso m/f Indirizzo e-mail Provincia di residenza Nominativo, codice fiscale, indirizzo o altri elementi di identificazione personale Dati di contatto (numero di telefono, e-mail, ecc.) Anamnesi familiare Diario visite Diario clinico Patologie attive, pregresse e sospette Prescrizioni farmaceutiche Prescrizioni di laboratorio e specialistiche Esiti di prescrizioni di laboratorio e specialistiche con eventuali allegati Vaccinazioni Esenzioni per reddito o patologia Registrazioni somatometriche Dati pressori Scadenziario Allergie ed intolleranze	Interessati Colleghi in forma associata Assistenti di studio Medici in formazione Personale infermieristico Distretti, ASL, Aziende ospedaliere e Regioni	10 anni a decorrere dalla data di cessazione del rapporto d'assistenza (revoca - decesso) Data di inizio del trattamento: 22-05-2018

Trattamento:	Descrizione:	Finalita':	Categorie:	Dati personali:	Destinatari:	Conclusione:
Contabilita'	Il trattamento ha per oggetto le attivita' di gestione delle fatture attive e passive e di ogni documento relativo a clienti/pazienti e fornitori. Gestione dei rapporti con istituti bancari e assicurativi. Gestione della prima nota di cassa e in generale di cespiti, assicurazioni, etc. Gestione della tempistica dei pagamenti ai fornitori ed ai pazienti. Trasmissione dei documenti contabili agli specialisti del settore come i commercialisti organizzati secondo le forme previste dalla legge.	Tenuta dei registri contabili (art. 2214 c.c. e DPR 633/72) Adempimenti fiscali (TUIR D.P.R. 917/86 e SMI ed ogni altra normativa di settore)	Pazienti Personale dipendente Fornitori Consulenti e liberi professionisti, anche in forma associata	Codice fiscale ed altri numeri di identificazione personale Dati sanitari inerenti la prestazione Nominativo, indirizzo o altri elementi di identificazione personale Attivita' economiche, commerciali, finanziarie, assicurative Dati di contatto (numero di telefono, e-mail, ecc.) Coordinate bancarie	Societa' e imprese Consulenti e liberi professionisti in forma singola o associata Distretti, ASL, Aziende ospedaliere e Regioni	10 anni a decorrere dalla data fine del trattamento (art. 2220 codice civile che prevede la conservazione per 10 anni delle scritture contabili; art. 22 del D.P.R. 29 Settembre 1973, n.600) Data di inizio del trattamento: 22-05-2018

Il Considerando 75 del GDPR introduce il **concetto di rischio**:

"I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati".

Tipi di rischio, in forma meramente esemplificativa:

- **Trattamento (raccolta) di dati non necessario in base alla finalità**
  art. 5, par. 1 lett. b) (principio di finalità), art. 13
- **Informativa e termini non chiari o trasparenti**
  art. 4, par. 11 (consenso dell'interessato) e art. 13
- **Dati personali non aggiornati o obsoleti**
  art. 15 e 16 (diritto di rettifica)
- **Perdita di dati lato operatore**
  art. 32 (misure di sicurezza)
- **Inefficace o intempestiva cancellazione dei dati personali**
  art. 17 (diritto alla cancellazione)
- **Condivisione di dati con terze parti**
  art. 7 (condizioni per il consenso), inoltre anche art. 21 (diritto di opposizione) e 22 (processi decisionali automatizzati)
- **Trasferimento dati non sicuro**
  art. 32 (misure di sicurezza)
- **Comunicazione non tempestiva delle violazione di dati**
  art. 33 e 34 (notifica violazione dati e comunicazione all'interessato)
- **Vulnerabilità delle applicazioni web**
  art. 32 (misure di sicurezza)

L'art. 5, par. 1, lett. f), stabilisce che i dati devono essere "*trattati in maniera da garantire un'adeguata* ***sicurezza*** *dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («****integrità*** *e* ***riservatezza****»)*", quindi è **l'intero trattamento a dover essere sicuro**, non solo i dati come prodotto finale. Ciò comporta anche che le valutazioni di sicurezza vanno sviluppate per ogni tipo di trattamento e devono essere aggiornate in relazione alla circostanze, anche sopravvenute

Misure di sicurezza fisiche

Per approntare delle misure di sicurezza è necessario valutare fattori quali:

- la qualità delle porte e delle serrature e la protezione dei locali con allarmi, illuminazione di sicurezza o CCTV (telecamere);
- l'accesso ai locali e il controllo dei visitatori;
- il corretto smaltimento dei rifiuti cartacei o elettronici;
- la sicurezza delle apparecchiature informatiche, in particolare i dispositivi mobili (è utile tenere un registro con l'indicazione delle risorse informatiche utilizzate per trattare dati, la loro ubicazione fisica e i permessi di accesso alle stesse).

Misure di sicurezza informatiche (o logiche)

Fattori da considerare per la sicurezza informatica:

- sicurezza della rete e dei sistemi di informazione (**sistemi di autenticazione**);
- sicurezza dei dati conservati nel sistema (**controlli di accesso**);
- sicurezza online (sito web o applicazioni online);
- sicurezza dei dispositivi, in particolare quelli personali se usati per motivi aziendali.

Grazie per l'attenzione