Breve riepilogo del Regolanento

GDPR Il regolamento europeo sul trattamento dei dati personali UE 2016/679

Il regolamento generale sulla protezione dei dati GDPR (General Data Protection Regulation) è un regolamento attuato dall'Unione Europea per uniformare la protezione dei dati delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali, ed entrerà in vigore il 25 Maggio 2018 e si applica ai dati dei residenti nell'Unione Europe a. Questo di fatto abrogherà le norme del codice per la protezione dei dati personali (la famosa legge sulla Privacy n. 196/2003) e ci si aspetta quindi una rettifica della vecchia legge Italiana.
A tutti gli stati membri UE si applicherà quindi un insieme unico di regole. Ciascuno stato membro istituirà un'autorità sovrintendente indipendente per dare udienza ai reclami, effettuare indagini, sanzionare le infrazioni amministrative, ecc. Nel caso dell'Italia tutto ciò spetterà al Garante della Privacy, il quale però per la verifica delle infrazioni, potrà avvalersi anche delle forze dell'ordine (con la vecchia 196/2003 solo lui poteva effettuare indagini sulle violazioni della privacy).
Di seguito una descrizione di come impatta il GDPR nello studio medico che utilizza dati personali, sia digitali ma sopratutto cartacei, perchè gli stessi principi valgono sempre e comunque per tutti i dati personali, sia che siano trattati in modalità informatica che, a maggior ragione, cartacea. Per approfondire si può visitare la gazzetta ufficiale europea.

Quali sono i dati da proteggere?

Con la nuova regolamentazione, il vecchio concetto di "dato sensibile" viene riassunto in: tutte le informazioni che identificano univocamente una persona fisica. Queste informazioni vanno protette e sono così suddivise:

- Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- Dati genetici: ereditati o acquisiti, ottenuti tramite analisi di DNA ed RNA da un campione biologico della persona fisica in questione.
- Dati biometrici: come l'immagine facciale, grazie ai quali è possibile identificare una ed una sola persona fisica.
- Dati sulla salute: sia fisica che mentale, passata, presente o futura, ma anche informazioni su servizi di assistenza sanitaria, laddove presenti, indipendentemente dalla fonte, quale, ad esempio, un medico.

Brevemente, cosa cambia?

Rispetto alla vecchia legge sulla Privacy, il GDPR è meno complesso e più semplice in termini di comprensione, in quanto non vengono imposte norme specifiche sul comportamento che deve essere adottato per la protezione dei dati, ma delle linee guida che però devono essere rispettate al 100%:

- Regole più chiare su informativa e consenso.
- Fissate norme rigorose per i casi di violazione dei dati (data breach).
- Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali (Data Loss Prevention e Disaster Recovery) in caso di incidente fisico o tecnico;
- Diritto alla rettifica, cancellazione e portabilità.
- Eventuale Nomina di un RDP (responsabile per la protezione dei dati).

Breve riepilogo del Regolanento

GDPR Il regolamento europeo sul trattamento dei dati personali UE 2016/679

Informativa e consenso per il trattamento dei dati

L'informativa sul trattamento dei dati (che va resa disponibile per la consultazione e non firmata dai pazienti) deve spiegare:

a) in che modo e per quale scopo verranno trattati i propri dati personali;
b) se il conferimento dei propri dati personali è obbligatorio o facoltativo;
c) le conseguenze di un eventuale rifiuto a rendere disponibili i propri dati personali;
d) a chi saranno comunicati o se saranno diffusi i propri dati personali;
e) chi è il titolare (solitamente il professionista o il legale rappresentante della società) e il responsabile del trattamento (nel caso di utilizzo dei nostri gestionali, si può indicare Caes Software, ma possono essere presenti anche altri soggetti).

Un valido consenso invece deve essere esplicitamente dato per la raccolta dei dati e per i propositi per i quali sono usati. Pertanto se la richiesta viene inserita nell'ambito di altre dichiarazioni essa va distinta e formulata con linguaggio semplice e chiaro. Condizione di validità del consenso è che le finalità per cui viene richiesto siano esplicite, legittime, adeguate e pertinenti (liceità del trattamento dei dati). Nel caso in cui il consenso al trattamento dei propri dati personali per una o più specifiche finalità sia stato espresso da minori esso è valido solo se il minore ha almeno 16 anni. Qualora il minore abbia un'età inferiore ai 16, il consenso al trattamento deve essere dato da un genitore o da chi eserciti la potestà, e deve essere verificabile.

Data breach o violazione dei dati

Il titolare del trattamento dei dati avrà l'obbligo legale di rendere note le fughe di dati (furti o violazioni) all'autorità nazionale e di comunicarle entro 72 ore da quando ne è venuto a conoscenza. In alcune situazioni le persone di cui sono stati sottratti i dati dovranno essere avvertite.

Perdita dei dati (Data Loss Prevention e Disaster Recovery)

Si parla di perdita di dati (data loss) nel caso in cui informazioni sensibili vengano effettivamente perse da un'azienda (o in qualche modo rese inaccessibili), quindi per Data Loss Prevention si intende la possibilità di prevenire o comunque recuperare la perdita di dati. Il Disaster Recovey invece è la possibilità di ripristinare tutte le informazioni in caso di gravi problemi (es. si verifica un danno irreparabile al PC server che contiene tutti i dati dei pazienti). Una perdita dei dati all'interno dello studio medico deve essere assolutamente evitato. Non è possibile chiedere ai pazienti di effettuare nuovamente esami oppure firmare di nuovo consensi. E' consigliabile quindi effettuare frequenti backup dei dati, differenziati per data e su dispositivi che non risiedano solo all'interno della rete e nella sede aziendale.

Diritto alla Rettifica, alla Cancellazione e Portabilità

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti, e altresì ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano (diritto all'oblio). Sono esclusi quei dati che servono per l'adempimento di un obbligo legale che richieda il trattamento previsto (ad esempio le fatture). L'interessato ha il diritto di ricevere in un formato leggibile da dispositivo automatico i dati personali che lo riguardano, come ad esempio una cartella clinica (diritto alla portabilità).

Breve riepilogo del Regolanento

GDPR Il regolamento europeo sul trattamento dei dati personali UE 2016/679

Eventuale nomina di un responsabile per la protezione dei dati (DPO o RDP)

Il responsabile per la protezione dei dati (RDP oppure in inglese DPO acronimo di Data Protection Officer) è una persona esperta di legislazione e pratiche relative alla protezione dei dati che deve assistere colui che li controlla o li gestisce al fine di verificare l'osservanza interna al regolamento. Il responsabile per la protezione dei dati è una figura che dovrebbe avere una buona padronanza dei processi informatici, della sicurezza dei dati e di altre questioni di coerenza aziendale riguardanti il mantenimento e l'elaborazione di dati personali e sensibili.

L'RDP può essere sia una figura interna che esterna alla struttura, però dovendosi confrontare e imporre le sue decisioni agli alti vertici, si consiglia di nominarne uno esterno in quanto privo di conflitti di interesse con i suoi diretti superiori.

La nomina di un RDP non è obbligatoria, dipende dall'entità dello studio medico. Consigliamo di effettuare qualche incontro con professionisti del settore per verificare l'eventuale necessità.

Chi è il responsabile in caso di qualsiasi violazione?

Il principale responsabile, che può essere quindi sanzionato in maniera diretta e personale in caso di violazioni o non attuazioni di procedure di protezioni adeguate, è sempre il Titolare del Trattamento dei Dati, che nelle piccole realtà coincide quasi sempre con il titolare della struttura stessa. In caso di violazione, a catena possono poi essere individuate altre figure che concorrono alla responsabilità. Per non rispondere del danno commesso derivante dal trattamento dei dati personali, il titolare del trattamento dei dati deve provare di aver fatto tutto il possibile per evitarlo.

Cosa cambia nei gestionali prodotti dalle Software House

I gestionali devono essere GDPR Compliance, ovvero hanno ottenuto una certificazione riguardo la conformità della disciplina interna aziendale rispetto alla normativa di recente introduzione all'interno dell'Unione Europea. Chi è già in possesso di questi software, deve sapere che ha uno strumento che può essere utilizzato tranquillamente affinché lo studio medico possa adempiere correttamente alla protezione dei dati informatici secondo le norme europee vigenti, perché:

1. Utilizzano database SQL non esposti all'esterno tramite Internet e che possono essere utilizzati tramite connessione TCP locali non accessibili da utenti non autorizzati.
2. Hanno una gestione degli operatori che consente di dare autorizzazioni speciali ai responsabili del trattamento e limitazioni ai vari incaricati dello studio.
3. Consentono cancellazioni così come previsto per il diritto all'oblio.
4. Consentono modifiche così come previsto per il diritto alla rettifica.
5. Consentono esportazioni in vario formato così come previsto per il diritto alla portabilità.
6. Attraverso copie di backup che lo studio deve effettuare autonomamente, è possibile ripristinare eventuali dati persi.

I database locali alla LAN non devono essere nè criptati nè pseudonominizzati; queste tecniche sono obbligatorie se i database fossero esposti all'esterno della propria LAN, tipo database in Cloud o su server remoti. Pertanto i dati locali dei gestionali non hanno protezione di criptatura ed è sufficiente applicare la protezione espresse nei punti sopra, al contrario tutti i dati che lo studio trasmette sui nostri database remoti di

Breve riepilogo del Regolanento

GDPR Il regolamento europeo sul trattamento dei dati personali UE 2016/679

www.spesasanitaria.it e www.clinicloud.it per l'invio al Sistema TS, la Fatturazione elettronica e l'App di comunicazione con il paziente, sono completamente criptati secondo sistemi tecnologicamente avanzati.

In definitiva cosa devo fare?

Prendere coscienza: questo è il primo passo da fare.

Abbiamo visto come Il GDPR prende in considerazione il dato personale sotto molteplici aspetti: sono dati personali sia quelli cartacei che quelli informatici, sono molto importanti le modalità di accesso e le misure in atto per proteggerli. Questo coinvolge tutta la struttura organizzativa dello studio o azienda.

La presa di coscienza può essere fatta solo aumentando la propria conoscenza, per cui una società specializzata in GDPR, un corso online, un corso gratuito organizzato da associazioni di categoria, potranno aiutarvi nel capire cosa fare. In generale se già si rispetta la normativa italiana sulla privacy, legge 196/2003, si è già un passo avanti.

Il regolamento Europeo è molto incisivo per le strutture che trattano big- data, per le strutture pubbliche, per le strutture sanitarie di grosse dimensioni. Le piccole strutture che fanno un uso del dato ai soli fini interni sono meno coinvolte nella complessità del GDPR ed è sufficiente poco per essere in regola con il regolamento Europeo.

Nel frattempo in attesa di ulteriori linee guida, il Garante della Privacy ha diffuso una guida sintetica al nuovo Regolamento che evidenzia "cosa cambia" e "cosa non cambia" dopo il 25 maggio.