XDENT
Odontoiatria

CompuGroup Medical

GDPR NELLO STUDIO DENTISTICO. L'ABC PER ORIENTARSI.

Comprendere le nuove disposizioni di legge europee sulla privacy non è semplice.
Ecco un vocabolario base per orientarti e comprendere.

Prendersi cura dei nostri pazienti, significa anche proteggerli e trattare i loro dati in maniera corretta, etica e professionale. Nonostante si faccia un gran parlare di privacy, leggi e regolamentazioni, sono in pochi quelli che sono veramente informati sulla questione. L'entrata in vigore del nuovo regolamento europeo sul trattamento dei dati personali (**GDPR**) ha risollevato argomenti importanti ma che, nella maggior parte dei casi, finivano spesso in fondo alla lista delle priorità dello studio dentistico.

Il trattamento dei dati in ambito sanitario, in particolare, costituisce uno dei contesti più delicati proprio per la natura "**sensibile**" dei dati che riguardano lo stato di salute degli interessati, dati rispetto ai quali l'aspettativa di riservatezza è, tradizionalmente, molto elevata.

Abbiamo raccolto qui, in forma di vocabolario, i termini e le indicazioni più importanti del **GDPR** per aiutarvi a comprendere la documentazione che troverete online.

Accountability: il principio espresso nel nuovo regolamento che prevede che il titolare del trattamento dei dati sia in grado di dimostrare di aver adottato in modo **attivo** un sistema di misure per proteggere i dati personali.

Breach (Data breach): il nuovo **GDPR** prevede l'obbligo di dare comunicazione all'autorità di controllo competente di eventuali attacchi informatici con violazioni dei dati personali entro il tempo massimo di 72h.

Consenso: in base al nuovo Regolamento Generale (art. 4 **GDPR**), si intende per consenso qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante **dichiarazione o azione inequivocabile**, al trattamento dei dati personali che lo riguardano. Con azione si intende la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Il consenso quindi non si esprime più con il silenzio, l'inattività o la preselezione di caselle.

Deletion (Data deletion): **il paziente può richiedere di eliminare od oscurare i dati che lo riguardano**. In ambito sanitario si rivela in questo caso una situazione particolare perché per legge è necessario conservare alcuni dati per un certo numero di anni per questioni medico/legali. In questo caso quindi è preferibile oscurare il dato.

Guida del Garante italiano: l'Autorità di controllo italiana (Garante Privacy) ha pubblicato una Guida (link) che offre un **panorama delle principali problematiche** che imprese e soggetti pubblici dovranno tenere presenti in vista della piena applicazione del regolamento.

Information obligation: per prepararsi all'arrivo del **GDPR** è necessario informare correttamente e in maniera comprensibile i pazienti del trattamento dei dati e dei loro diritti di rettifica, cancellazione o oblio.

Misure di sicurezza: le misure di sicurezza che lo studio dentistico deve adottare devono "**garantire un livello di sicurezza adeguato al rischio**" del trattamento. Non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza.

One stop shop: il nuovo Regolamento europeo per la protezione dei dati personali introduce il **principio dello sportello unico** (one stop shop). Tale principio stabilisce che le imprese avranno a che fare con una sola Autorità di vigilanza (Garante Privacy), cioè quella del paese dove hanno la sede principale.

Portability (Data portability): il paziente può richiedere, e deve poter ottenere, una **copia dei propri dati in un formato elettronico interscambiabile**, ad esempio il formato 'XML'.

Privacy by design: si tratta di un approccio concettuale innovativo che impone alle aziende l'obbligo prevedere fin da subito gli **strumenti a tutela dei dati dei pazienti**.

Questo nella pratica significa:

- prevenire non correggere, valutare i problemi di gestione dei dati all'inizio del progetto;
- privacy come impostazione di default;
- privacy incorporata es. l'utilizzo di tecniche di pseudonimizzazione o minimizzazione dei dati;
- sicurezza durante tutto il ciclo del prodotto o servizio;
- trasparenza;
- centralità dell'utente.

Registro dei trattamenti: Il nuovo regolamento europeo sul trattamento dei dati personali **impone che chi applica un qualsiasi trattamento sui dati** tenga un registro delle attività di trattamento svolte (Art. 30 **GDPR**). Si tratta di un registro dove vengono rendicontati i processi e le attività svolte sui dati dei pazienti, quindi chi ha interagito con quel documento.

Responsabile della protezione dei dati: si tratta di una nuova figura introdotta proprio dal **GDPR**. É la **persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento** (vedi sotto). Si tratta di un soggetto, distin-

to dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.

Sub-responsabile: il responsabile del trattamento (vedi sopra) può ricorrere ad un altro responsabile solo se è stato previamente autorizzato (tramite il contratto) dal titolare. Il sub-responsabile dovrà essere nominato tramite contratto o atto giuridico e nel rispetto degli obblighi imposti al primo responsabile del trattamento. **E' il primo responsabile che risponde dell'inadempimento dei sub-responsabili**, nei confronti del titolare, a meno che non riesca a dimostrare che il danno non è in alcun modo imputabile a lui. Per questo motivo il responsabile deve sempre avvisare il titolare della nomina o modifica di un sub-responsabile.

Traceability (Data traceability): è il d**iritto di sapere dove vengono conservati i dati**. Non tutti potrebbero essere favorevoli al fatto che i propri dati risiedano in un cloud o in un server fuori dall'Italia.

Titolare del trattamento: il Titolare del trattamento (data controller) è colui che "**da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali**". In sostanza il titolare è colui che tratta i dati senza ricevere istruzioni da altri, colui che decide "perché" e "come" devono essere trattati i dati. Il titolare del trattamento non è, quindi, chi gestisce i dati, ma chi decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali, compreso l'obbligo di notifica al Garante nei casi previsti.

La soluzione per adeguare il tuo studio dentistico al GDPR

La nuova versione **Xdent 9.0** è un valido e completo ausilio che consente, con semplicità, di avere indicazioni per essere in regola rispetto alle prescrizioni del **GDPR**, limitando il rischio di sanzioni in caso di controllo. Inoltre, nell'eventuale casistica di attacco informatico, la soluzione permette di avere un supporto utile a dimostrare che è stato condotto un atteggiamento proattivo per la gestione della sicurezza.

Vieni a conoscerla.

www.xdent.it