Come prendersi cura dei dati personali dei propri pazienti

Gli adempimenti pratici che scaturiscono dalla normativa europea sulla protezione dei dati personali per i medici e gli odontoiatrici

Le professioni sanitarie sono senza dubbio uno degli ambiti maggiormente interessati dall'entrata in vigore del Regolamento Europeo 2016/679 sulla protezione e libera circolazione dei dati personali, delle persone fisiche e dalla recente armonizzazione del Codice Privacy, ad opera del D. Lgs n. 101/2018. Queste norme richiedendo una serie di adempimenti e misure da implementare all'interno delle organizzazioni degli studi medici e delle strutture sanitarie e impattano dal punto di vista gestionale, decisionale ed economico sulla professione.

In un sistema sanitario sempre più interconnesso in cui i dati personali dei pazienti sono trattati attraverso molteplici strumenti (fascicolo sanitario elettronico, sistemi di diagnostica, telemedicina, dispositivi medici, ecc.) il pieno rispetto dei principi di protezione dei dati personali è un dovere fondamentale per il corretto svolgimento della professione medica, come peraltro previsto dal Codice di deontologia medica del quale si riportano gli articoli salienti:

Art. 9 Segreto professionale (stralcio)

"Il medico deve mantenere il segreto su tutto ciò che gli è confidato o che può conoscere in ragione della sua professione; deve, altresì, conservare il massimo riserbo sulle prestazioni professionali effettuate o programmate, nel rispetto dei principi che garantiscano la tutela della riservatezza."

Art. 10 Documentazione e tutela dei dati (stralcio)

"Il medico deve tutelare la riservatezza dei dati personali e della documentazione in suo possesso riguardante le persone anche se affidata a codici o sistemi informatici. Il medico deve informare i suoi collaboratori dell'obbligo del segreto professionale e deve vigilare affinché essi vi si conformino."

Art. 11 Comunicazione e diffusione di dati

"Nella comunicazione di atti o di documenti relativi a singole persone, anche se destinati a Enti o Autorità che svolgono attività sanitaria, il medico deve porre in essere ogni precauzione atta a garantire la tutela del segreto professionale. Il medico, nella diffusione di bollettini medici, deve preventivamente acquisire il consenso dell'interessato o dei suoi legali rappresentanti. Il medico non può collaborare alla costituzione di banche di dati sanitari, ove non esistano garanzie di tutela della riservatezza, della sicurezza e della vita privata della persona."

Da qui la necessità per il medico di porre attenzione ai dati personali dei propri pazienti, inserendo la protezione dei dati all'interno del processo di cura, ciò significa, da una parte salvaguardare il paziente limitando gli errori che possono derivare da un'errata o superficiale gestione a tutti i livelli funzionali della propria organizzazione, dall'altra preservarlo dai rischi di un discriminato utilizzo e conoscenza delle informazioni che lo riguardano.

Tra le principali novità apportate dal GDPR si sottolineano:

- l'intensificazione dei doveri che gravano sui Titolari del trattamento dei dati (medico libero professionista, società tra professionisti, struttura sanitaria ecc…);
- l'introduzione del principio di *accountability* (l'autonomia di fare scelte sulle misure di sicurezza con la necessità di comprovarle);

- l'irrobustimento delle garanzie di sicurezza e di riservatezza per i dati personali nel passaggio dalle misure minime alle misure adeguate;
- la necessità di aggiornare le informative sul trattamento dei dati personali e rivedere le basi giuridiche dei trattamenti;
- la necessità un riesame della propria organizzazione interna ed esterna: nomine dei dipendenti secondo un adeguato sistema di autorizzazione, nomina dell'amministratore di sistema e le nomine dei responsabili esterni cioè di coloro che trattano dati personali per conto del professionista (*software house* e servizi *cloud* ad es.);
- per le strutture ove lavorano in sinergia più professionisti, la necessità di analizzare i rapporti con i colleghi di studio e l'impatto di questa disciplina su tali rapporti: accordi di contitolarità, regole e procedure comuni da inserire in manuali di gestione di studio, sperimentando i principi del Regolamento della *privacy by design* (tutela del dato personale fin dalla progettazione) e *privacy by default* (regole predefinite di rispetto della norma e delle misure adottate attraverso procedure interne);
- l'introduzione dei registri dei trattamenti e delle violazioni;
- gli adempimenti in caso di data breach;
- il rafforzamento dei diritti degli interessati;
- l'inserimento nel nostro paese della figura del Data Protection Officer;
- il ricorso a regole deontologiche o alla certificazione nei processi di trattamento;
- l'inasprimento sanzionatorio amministrativo e il mantenimento anche delle sanzioni penali per volontà del legislatore italiano, non presenti nel Regolamento.

Chi è tenuto a conformarsi alla normativa e con quali responsabilità?

Colui che esercita la professione - singolarmente o insieme ad altri professionisti - prendendo le decisioni sui mezzi e le finalità del trattamento di dati personali, è definito dal Regolamento Titolare del Trattamento dei dati personali.
Per coloro che svolgono l'attività in forma associata, in forma stabile e continuativa, potrebbe configurarsi la necessità di sottoscrivere un accordo di Contitolarità del trattamento dei dati, per legittimare il trattamento in comune dei dati, condividere misure di protezione e procedure.
Tutti i professionisti - anche se non usano il personal computer - sono tenuti al rispetto della normativa trattando dati personali dei loro pazienti e sugli stessi gravano i doveri e responsabilità derivanti dalla normativa sulla protezione di tali dati.
E' utile ricordare anche che, nel Regolamento scompare la distinzione basata sulla natura pubblica o privata dei soggetti che trattano i dati avendone responsabilità, rilevando unicamente la finalità del trattamento perseguita, vale a dire se la finalità concerne un interesse pubblico o privato. L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri potrà essere posta in essere a prescindere dalla natura soggettiva di chi la compie.

Chi sono i soggetti interessati dal trattamento dei dati da parte del medico?
I soggetti interessati al trattamento dei dati da parte di un medico sono i suoi pazienti e in taluni casi anche i familiari dello stesso. Anche i dati dei defunti ricevono una protezione dal nostro Codice Privacy. Ma non solo: il medico potrebbe gestire anche dati personali del proprio personale dipendente o dei suoi collaboratori o dei propri fornitori.

In che termini devono essere aggiornate le informative sul trattamento dei dati?

Il primo obbligo per il medico, indipendentemente dalle dimensioni del proprio studio professionale, è quello di informare il paziente, con linguaggio semplice e chiaro e tale da rendere agevolmente comprensibili gli elementi indicati negli articoli 13 e 14 del Regolamento che sono in sintesi:

- i dati di contatto del Titolare del trattamento e del DPO se nominato
- le finalità del trattamento (finalità di cura, diagnosi, assistenza, terapia ecc..)
- le basi giuridiche del trattamento (consenso, contratto di cura, le finalità di rilevante interesse pubblico)
- periodo di conservazione dei dati
- a chi vengono comunicati i dati (dentro e fuori la propria struttura)
- una chiara esplicazione del diritto di accesso e degli altri diritti degli interessati e la modalità per esercitarli.

Per il trattamento dei dati nell'ambito sanitario il Codice Privacy italiano ha previsto delle modalità particolari per informare l'interessato e per il trattamento dei dati personali. Le informazioni date ai pazienti possono essere integrate con appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico (nella sala di attesa) affissi e diffusi anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica, in particolare per quanto riguarda attività amministrative effettuate per motivi di interesse pubblico rilevante che non richiedono il consenso degli interessati (questo in particolar modo è valido per i MMG e i pediatri di libera scelta ma anche per le strutture sanitarie pubbliche e private).

Le informazioni possono essere fornite per il complessivo trattamento dei dati personali necessario per attività di diagnosi, assistenza e terapia sanitaria anche se devono analiticamente, essere evidenziati eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati:

1. per fini di ricerca scientifica e nell'ambito di sperimentazioni cliniche, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;
2. nell'ambito della teleassistenza o telemedicina;
3. per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica;
4. ai fini dell'implementazione del fascicolo sanitario elettronico di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179

L'informativa va fornita al momento in cui i dati sono ottenuti o raccolti dal medico, per iscritto o con altri mezzi anche elettronici, ovvero se richiesto dall'interessato le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato. Scelta questa che spetta al medico dopo attenta valutazione delle caratteristiche della propria organizzazione.

Lo studio medico dovrà consegnare con le stesse modalità anche ai propri collaboratori e ai fornitori le opportune informative.

Quali categorie di dati può trovarsi a trattare il medico?

Il medico si trova, nella quotidiana attività professionale, a dover trattare, per la maggior parte, **dati relativi alla salute**, che per definizione sono quelli "*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*" - ricompresi nella più vasta categoria dei dati cosiddetti "particolari" - definizione questa che sostituisce la più conosciuta di "dati sensibili". Ovviamente tratterà anche dati identificativi cosiddetti "comuni" e raramente dati giudiziali.

Ma il consenso al trattamento dei dati è l'unica base giuridica su cui si fonda il trattamento dei dati particolari per il medico?

La risposta alla domanda è no, nel senso che il consenso è una tra le altre condizioni di liceità del trattamento di categorie particolari di dati.

Il consenso quando è richiesto dal medico al paziente, deve essere prestato da quest'ultimo in forma esplicita (non necessariamente scritta) per una o più finalità specifiche ed essendo una manifestazione libera di volontà come tale, in linea generale, è sempre revocabile. Tale revoca non pregiudica la liceità del trattamento eseguito prima della revoca stessa. Quando il medico ha valutato che per la specifica finalità, il trattamento dei dati particolari del paziente debba basarsi sul consenso del paziente, è sul professionista stesso che grava l'onere di dimostrare che l'interessato ha prestato il proprio consenso.

Se lo studio intende utilizzare i dati per finalità diverse e ulteriori rispetto a quelle di cura (ad esempio: per pubblicare i dati del paziente su riviste scientifiche o a congressi oppure per inviare newsletter periodiche informative) sono necessari ulteriori e differenziati consensi.

Il Regolamento prevede ulteriori condizioni di liceità quali la necessità di tutelare un interesse vitale dell'interessato o di altro persona fisica qualora l'interessato si trovi nella incapacità fisica o giuridica di prestare il proprio consenso.

Inoltre, stabilisce che se il trattamento di dati relativi alla salute è necessario per motivi di interesse pubblico rilevante, il trattamento non necessiti di consenso esplicito dell'interessato anche se, tale trattamento, deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali degli interessati.

Il Codice Privacy, novellato, prevede che si consideri rilevante, l'interesse pubblico relativo ai trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, quali i: "*compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica*". Sul punto rimane quindi nodale la valutazione, da parte del sanitario, sulla base giuridica su cui si fondi il trattamento dei dati dei propri pazienti.

Così come espressamente il Regolamento non prevede la necessità del consenso per il trattamento dei dati per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità.

Fondamentale per la professione medica è il rimando che il Regolamento fa al segreto professionale e al trattamento di dati particolari, quando tali dati sono trattati sotto la responsabilità di un professionista soggetto al segreto professionale, conformemente alle norme statali o a quelle stabilite dagli organismi nazionali competenti (rimarcando per i professionisti i doveri posti dal proprio Codice Deontologico). Fa riflettere la formula del giuramento di Ippocrate **Deliberato da FNOMCeO il 23 marzo 2007** che così recita « *giuro di osservare il segreto professionale e di tutelare la riservatezza su tutto ciò che mi è confidato, che vedo o che ho veduto, inteso o intuito nell'esercizio della mia professione o in ragione del mio stato*».

Il Regolamento, però, lascia agli Stati membri la possibilità di "mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute" (cosiddetta "riserva"). In tal senso il legislatore italiano ha previsto, con il Codice Privacy novellato l'emanazione di **misure di garanzia**, fissate dall'autorità di controllo

nazionale (Garante della Privacy) e riviste a cadenza biennale. Quindi, il Garante dovrà adottare delle misure di garanzia, sentito il Consiglio superiore di sanità e tenendo conto delle linee guida, delle raccomandazioni e delle buone prassi del Garante Europeo, in particolare con riferimento alle cautele relative alle "modalità per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute, alla prescrizione di medicinali e ai profili organizzativi e gestionali in ambito sanitario. Le misure di garanzia individueranno le misure di sicurezza, ivi comprese tecniche di cifratura e di pseudonimizzazione, misure di minimizzazione, specifiche modalità di accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché eventuali altre misure necessarie a garantire i diritti degli interessati."
Momento fondamentale per tutto il settore sanitario sarà quindi l'emanazione e la discussione delle misure di garanzie del Garante italiano che dovranno previamente essere sottoposte a consultazione pubblica per un tempo non inferiore a 60 giorni.
Inoltre l'autorità di controllo dovrà farsi promotrice anche delle regole deontologiche per il trattamento dei dati relativi alla salute.

Quali misure di sicurezza deve adottare il medico?

Il Regolamento Europeo impone di adottare non più misure di sicurezza minime uguali per tutti, ma richiede ai Titolari del trattamento di approntare e mettere in atto misure tecniche e organizzative adeguate, per garantire ed essere in grado dimostrare che il trattamento è effettuato conformemente al Regolamento. Le misure dovranno essere tarate sulle caratteristiche dello studio, sia in termini di sicurezza fisica (luoghi e ambienti) che organizzativa (nomine, sistema di autorizzazione, policy di studio) che informatica (strumenti informatici e soluzioni hardware e software adeguati). Il Titolare dovrà monitorare e aggiornare periodicamente le misure scelte e le procedure per evitare i rischi di Data Breach (violazione o perdita anche accidentale di dati) nell'ottica della tutela della riservatezza "al massimo grado".

Le misure di protezione informatica hanno una rapida evoluzione tecnologica, per cui è opportuno che il medico possa contare su un consulente informatico di propria fiducia, che dovrebbe nominare amministratore di sistema, per rendere il suo computer e la sua rete sempre protetto per prevenire le minacce informatiche quantomeno più frequenti.

Nel caso di trattamento dei dati in forma cartacea, il medico dovrebbe istituire delle schede sanitarie per ogni singolo paziente nelle quali conservare il modulo di consenso firmato e ogni altro atto e documento inerente la salute del paziente. Le schede dovrebbero essere conservate in un luogo e in un modo tale da evitare che persone non autorizzate ne possano prendere conoscenza. Le schede dovrebbero essere conservate in un luogo e in un modo tale da evitare che persone non autorizzate ne possano prendere conoscenza. Per esempio, se sono riposte in un armadio, questo dovrebbe essere chiuso a chiave e collocato in una stanza dello studio non accessibile al pubblico in generale. Le chiavi dell'armadio dovrebbero essere in possesso solo del medico e del suo sostituto (o dei suoi collaboratori medici) e non di altre persone.

L'organizzazione dello studio: quali adempimenti

Le misure di sicurezza non possono prescindere da una corretta organizzazione in termini di incarichi, ripartizione della responsabilità e consapevolezza delle misure e delle procedure da adottarsi secondo una visione sostanzialistica della normativa.

Se il medico, nel proprio studio, si avvale di collaboratori o sostituti o personale infermieristico o di personale di segreteria deve redigere una lettera di nomina dei soggetti autorizzati al

trattamento, che si devono attenere alle istruzioni impartite dal Titolare del trattamento. Tale istruzioni non possono prescindere da una attività formativa del personale, che dovrà essere anche responsabilizzarlo, attraverso un regolamento o un manuale di procedure sulla protezione dei dati e sull'uso corretto degli strumenti informatici che può assurgere anche a codice disciplinare per il personale dipendente. Deve essere valorizzata e costantemente adeguata la formazione del personale di segreteria, che deve essere consapevole dei comportamenti più adeguati a tutela della privacy.

Tutto ciò deve avvenire costantemente e deve sostanziarsi in una serie di attività specifiche e dimostrabili, con monitoraggi periodici.

Se il medico si avvale di tecnici, consulenti e fornitori esterni che trattano per suo conto i dati personali dei suoi pazienti (commercialista per la tenuta della sua contabilità, l'amministratore di sistema, società fornitrici di software gestionali di studio ecc…), questi **dovranno essere nominati responsabili esterni del trattamento art. 28.** La nomina prevista dall'art. 28 del Regolamento, richiede non solo che alla base del rapporto vi sia un contratto scritto con il fornitore, ma che lo stesso risponda in solido per l'intero, con il Titolare del trattamento, in caso di richieste risarcitorie provenienti da soggetti che si ritengano lesi nei loro diritti fondamentali alla riservatezza, alla salute, alla libertà.

Quali sono i diritti degli interessati?

Il paziente ha diritto in ogni momento di sapere se è in corso un trattamento di dati che lo riguardano e se confermato - di ottenere una copia di tali dati ed essere informato su: l'origine dei dati, i destinatari dei dati, le finalità del trattamento, l'esistenza di un processo decisionale automatizzato, compresa la profilazione, il periodo di conservazione dei dati. Il paziente potrebbe chiedere che i dati personali a lui riferiti siano rettificati o cancellati o che ne venga limitato il trattamento (es. chiedendo l'oscuramento) ovvero potrà opporsi al trattamento dei dati personali per motivi connessi alla sua situazione particolare che deve specificare nella richiesta. Così come potrà rivolgersi, in caso non sia soddisfatto delle risposte ricevute dall'esercizio del suo diritto di accesso, di rivolgersi al Garante per la protezione dei dati personali, mediante un reclamo ai sensi dell'art. 77 del Regolamento, oppure all'autorità giudiziaria. Le richieste del paziente vanno valutate nella loro fondatezza e va data una risposta in caso di esercizio di accesso agli atti nei primi 30 giorni.

Il medico deve tenere un Registro dei Trattamenti?

Il Registro, previsto dal Regolamento Europeo, è un documento che contiene le principali informazioni sulle attività di trattamento dei dati personali e rappresenta un quadro delle attività svolte all'interno dell'organizzazione o dello studio professionale indispensabile per la valutazione del rischio.

Il Registro è obbligatorio per tutte le organizzazioni che abbiano almeno 250 dipendenti, ma lo è anche per qualunque Titolare che tratti dati particolari come quelli relativi alla salute, indipendentemente dal numero dei dipendenti, per cui in sostanza **è obbligatorio per i medici**.

L'Autorità Garante per la Privacy ha messo a disposizione sul proprio sito internet un **modello semplificato del Registro dei Trattamenti** da utilizzare per le PMI - piccole e medie imprese e per i professionisti. Il modello predisposto dal Garante tiene conto delle realtà di ridotte dimensioni organizzative e per questo motivo viene proposto in forma semplificata, di più agile compilazione e tenuta. Nel registro si elencano le tipologie di trattamenti che vengono svolti dallo studio e che coinvolgono i dati personali degli interessati. Ogni professionista deve esplicitare chiaramente da chi e come saranno trattati i dati, dall'informativa all'archiviazione, ma non va visto come un mero adempimento burocratico, bensì parte integrante di un sistema di corretta gestione dei dati personali, in quanto finalizzato a tenere sotto controllo il ciclo vitale del dato.
E' un documento che può essere necessario esibire agli organi di controllo in caso di verifiche o accertamenti.

Il contenuto del registro è il seguente:

- dati identificativi e di contatto del Titolare del trattamento, dei contitolari (se esistenti) e del DPO (se nominato);
- le finalità del trattamento (ad esempio: rapporto di cura, finalità di ricerca);
- la base giuridica su cui si fonda il trattamento (ad esempio: obbligo legale oppure consenso dell'interessato);
- la categoria degli interessati (ad esempio: pazienti, dipendenti)
- la categoria dei dati trattati (ad esempio: identificativi, relativi alla salute)
- la fonte dei dati personali (ad esempio: conferiti direttamente dall'interessato o acquisiti dal suo FSE);
- la tipologia del trattamento (raccolta di dati del nuovo paziente, utilizzo del software informatico gestionale per il trattamento dei dati);
- le categorie di destinatari a cui i dati possono o devono essere comunicati (ad esempio: ASL, Agenzia delle Entrate, ASL, Enti previdenziali ed assistenziali Autorità Giudiziaria, Compagnie Assicurative, ecc.);
- gli eventuali responsabili esterni (ad esempio: il fornitore informatico o il commercialista)
- i Paesi stranieri verso cui i dati possono essere trasferiti fuori UE;
- il periodo di conservazione dei dati (ad esempio: 10 anni o comunque per il tempo necessario a tutelare il diritto di difesa del titolare);
- le misure di sicurezza fisiche, organizzative ed informatiche adottate per la protezione dei dati;

In contesti in cui lo studio medico viene nominato responsabile esterno del trattamento potrebbe essere necessaria la predisposizione di un registro dei trattamenti per il titolare e uno per il responsabile del trattamento dei dati.

Il modello semplificato è scaricabile sul sito del Garante: https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.

Il registro delle violazioni e il data breach, cosa sono?

Il termine data breach indica ogni 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 in archivi cartacei o in archivi informatici. La gestione del data breach richiede la presenza di una procedura di studio che definisca i principi e

le azioni per gestire la violazione dei dati personali, così da poter adempiere agli obblighi relativi alla annotazione dell'evento nel registro delle violazione e della eventuale notifica alla Autorità di Controllo e di comunicazione ai singoli interessati, obblighi previsti agli art. 33 e 34 del Regolamento.

Sulla base delle dimensioni dell'organizzazione sarà necessario formare un team, che dovrà essere avvisato in caso, anche solo, di una presunta violazione di dati personali. Questo team deve garantire la prontezza necessaria fornendo risposte immediate, efficaci ed esperte a qualsiasi sospetta o effettiva violazione dei dati personali. Il team deve essere composto dal Titolare del Trattamento, che si avvale di un gruppo multidisciplinare di persone competenti nel settore IT e legale (solitamente l'amministratore di sistema o comunque il referente per la materia) e il Dpo se nominato, che possono anche essere esterne all'organizzazione. Queste figure avranno il compito di dare un supporto al Titolare sulla valutazione del grado di probabilità che la violazione dei dati presenti un rischio effettivo per i diritti e le libertà delle persone interessate e di conseguenza per decidere:

- le eventuali misure tecniche ed organizzative assunte o da assumere per il contenimento della violazione o per prevenire in futuro violazioni simili;
- se è necessario effettuare la notifica art. 33 Regolamento all'Autorità di Controllo (Garante per la protezione dei dati) entro le 72 ore dalla scoperta della violazione;
- se è necessario effettuare la comunicazione agli interessati e stabilire quale possa essere il mezzo da utilizzare (comunicazione scritta, comunicazione pubblica o altro) e l'investimento da intraprendere;
- inserire nel registro delle violazioni dei dati, la descrizione violazione, con tutti i dati richiesti dall'art. 33 del Regolamento, in ogni caso, anche se dalla valutazione emergesse che non serve notificare al Garante e comunicare agli interessati la violazione.

IL DPO: è un obbligo per il medico incaricare questa figura?

Il Regolamento Europeo ha introdotto la figura del Responsabile della Protezione dei Dati (in inglese DPO). Si tratta di un soggetto, persona fisica o giuridica, nominato dal titolare con il compito di affiancarlo nella promozione della cultura della protezione dei dati e contribuire a dare attuazione agli elementi essenziali del Regolamento informando, dando consulenza e sorvegliando l'osservanza del Regolamento. Compito fondamentale di questa figura è la formazione e la sensibilizzazione del personale. Il DPO funge anche da punto di contatto con l'interessato e con l'Autorità Garante per la Privacy ed è per questo motivo che il suo nominativo va comunicato al Garante.

Il Regolamento Europeo non prevede specifici requisiti per svolgere la funzione di DPO. E' però necessario che sia un soggetto esperto in materia di protezione dei dati e del settore in cui opera, sia dal punto di vista legale e normativo, sia dal punto di vista tecnico-informatico. Per cui nella scelta del DPO è opportuno valutare attentamente il curriculum e/o le referenze del professionista o dell'azienda che si propone di svolgere tale attività quando si sceglie una figura esterna.

Tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati particolari, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici hanno l'obbligo di nominare un DPO, con l'unica oggi eccezione chiara, riguardo al trattamento di dati relativi alla salute svolto da un singolo professionista sanitario.

****

Con il presente intervento, lungi dall'essere un approfondimento esaustivo sulla materia, si è tentato di far comprendere che la protezione dei dati del paziente è parte del processo di cura ed è materia viva che deve essere conosciuta da tutti gli esercenti la professione medica e odontoiatrica. Sarà cura di questo Ordine dei Medici e degli Odontoiatri di tenere informati i propri iscritti sulla evoluzione della materia e dei relativi adempimenti. Con l'obiettivo di provare a rispondere ai dubbi e alle domande poste dai professionisti rispetto ai loro adempimenti, chiarendo a che la recente applicazione della normativa nell'ambito delle professioni sanitarie, impone al medico la prudenza nelle scelte spesso cruciali all'interno della propria organizzazione, auspicando che i prossimi interventi della nostra autorità Garante, dedicati alla sanità, siano il più vicini possibili nel tempo.

avv. Silvia Boschello

DPO dell'Omceo _____ della provincia di