CONSULENZA
L'informazione integrata per professionisti e aziende

ARTICOLI

ARTICOLO

Privacy

GDPR e studi medici: gli adempimenti di base per adeguarsi alle norme sul trattamento di dati personali

martedì, 27 novembre 2018

Ciascun medico nel proprio studio tratta dati personali e categorie particolari di dati personali, anche solo registrando il numero di telefono di un suo cliente o collega nella rubrica dello smartphone o semplicemente annotando il malessere accanto al nome del cliente nella sua agenda. Premesso ciò, vediamo quali sono le operazioni di base che un dottore deve effettuare per essere compliance con la nuova normativa sul trattamento dei dati, restando inteso che in tale materia non è possibile generalizzare, anche perché il nuovo principio dell'accountability, voluto dal legislatore europeo, obbliga ad analizzare in dettaglio e nel concreto ogni contesto in cui si verifica un trattamento di dati personali.

di: **Spedicato Annalisa**

Un medico nel suo studio effettua, senza ombra di dubbio, un trattamento di dati personali, anche se non ha dipendenti né collaboratori o non usa strumenti informatici. Non solo. Il professionista medico, tratta anche categorie particolari di dati personali. Se, infatti, nella prima tipologia di dati rientrano informazioni comuni che permettono di identificare direttamente o indirettamente una persona fisica, come anagrafiche, indirizzi email, numeri telefonici, indirizzi di residenza, matricola INPS e simili; nel secondo tipo di dati, rientrano informazioni più delicate, come dati sanitari, informazioni sulla razza, l'etnia, opinioni filosofiche, politiche, religiose, dati biometrici, dati genetici. Si comprende dunque come ogni medico si trova ad aver a che fare nella propria attività professionale con le suindicate tipologie di dati personali, considerando che, nel proprio quotidiano, può raccogliere, registrare, organizzare, conservare, consultare, elaborare, modificare, selezionare, estrarre, raffrontare, usare, interconnettere, bloccare,

comunicare, diffondere, cancellare e distruggere dati personali appartenenti a suoi clienti, fornitori, collaboratori, altri colleghi, manualmente e mediante strumenti informatici e telematici; tali operazioni sono infatti tutte quelle incluse nel concetto di "trattamento di dati personali" come definito nel Regolamento UE n. 679/2016 in materia di trattamento di dati personali (anche detto GDPR).

La fase di assessment o analisi

La prima cosa da fare per uno studio medico è quella di analizzare la propria organizzazione, individuando quali dati vengono trattati, scindendo quelli comuni dalle categorie particolari di dati, individuando a chi appartengono i dati trattati (generalmente pazienti, fornitori, colleghi, dipendenti), il proprio modo di operare sui dati personali trattati, gli strumenti utilizzati per il trattamento (elettronici o manuali), il contesto, i "percorsi" dei dati (dove sono raccolti, come sono comunicati all'interno dello studio e all'esterno, dove sono archiviati, per quanto tempo, quando e come sono distrutti, chi vi ha accesso), i soggetti terzi cui vengono eventualmente comunicati e con cui vengono condivisi.

Fatte queste operazioni, il medico avrà già un quadro più chiaro della propria situazione rispetto ai dati trattati; si tratta, infatti, di attività che gli torneranno utili anche nella predisposizione del Registro dei trattamenti, in cui tali informazioni dovranno poi essere riportate in maniera ordinata, secondo quanto stabilito dal Regolamento all'art. 30.

Le informazioni da rendere ai pazienti e l'informativa alle altre categorie di interessati

Avendo individuato i soggetti di cui si trattano i dati (cosiddetti interessati), il medico dovrà rendere a tutti un'informativa adeguata il cui contenuto sarà diverso a seconda del soggetto, in quanto innanzitutto la finalità del trattamento sarà diversa da soggetto a soggetto, quindi l'informativa da rendere ai pazienti avrà certamente delle informazioni differenti rispetto a quella indirizzata a dipendenti, collaboratori/colleghi, fornitori, altre persone. A tal proposito, si ricorda che l'art. 78 e seguenti del Codice in materia di trattamento dati personali (D. Lgs. n. 196/2003) come novellato dal decreto n. 101/2018, per il medico di medicina generale o pediatra di libera scelta (ma anche per le strutture pubbliche e private che erogano prestazioni sanitarie e socio sanitarie) definiscono delle regole più specifiche nel trattamento dei dati personali dei pazienti, ad esempio, in relazione all'informativa da rendere ai pazienti, l'art. 78 del novellato decreto parla di informazioni e non di informativa, sebbene il contenuto sia sempre quello stabilito dall'art. 13 del GDPR; il termine informativa invece ritorna quando si fa riferimento ai dati di fornitori, collaboratori/colleghi, dipendenti, altri soggetti.

Ma quali sono le "informazioni" che il medico dovrà rendere ai pazienti?

Secondo quanto stabilito all'art. 13 del GDPR, le informazioni, che vanno rese nel momento della raccolta del dato e dovranno essere formulate in un linguaggio semplice e chiaro preferibilmente in forma scritta (si veda l'art. 78 comma 3 decreto n. 196/2003 novellato), dovranno riguardare:

i) i dati di contatto del Titolare del trattamento, quindi del professionista titolare dello Studio; ii) i dati di contatto del/i Responsabile/i del trattamento dei dati (se presenti); iii) la/le finalità del trattamento dei dati; iv) le modalità di trattamento dei dati; v) il tempo di conservazione dei dati; vi) i soggetti a cui i dati vengono comunicati; vii) l'eventuale trasferimento all'estero dei dati; viii) i diritti dell'interessato (diritto di richiedere informazioni sul trattamento, diritto di accesso, modifica, opposizione, cancellazione, limitazione, portabilità dei dati, diritto di proporre reclamo all'Autorità di controllo) e come egli potrà esercitarli nei confronti del titolare; ix) i dati di contatto del Responsabile della protezione dei dati - DPO (se si rientra nei casi in cui è obbligatoria la nomina, ma per un piccolo studio professionale generalmente non è necessario).

Le suindicate informazioni devono essere riportate anche nell'informativa da rendere a colleghi, collaboratori, dipendenti, fornitori e altri soggetti, naturalmente definendo con precisione il contenuto.

Ora, soffermandosi alle informazioni da fornire ai pazienti, circa la/le finalità di trattamento dovranno essere menzionati gli scopi del trattamento dei dati, ovviamente la finalità di trattamento principale è quella di fornire il servizio di prestazione sanitaria richiesto dal paziente che per un medico si sostanzia nell'individuazione della malattia, quindi nella diagnosi, nell'assistenza e nella terapia sanitarie, nella riabilitazione o cura; oltre a tale finalità, ve ne sono da individuare altre strettamente connesse alla principale, come il trattamento dei dati per la comunicazione degli stessi - obbligatoria per legge - ad enti pubblici o autorità (si pensi alla comunicazione dei dati al sistema tessera sanitaria dell'Agenzia delle Entrate) o per la difesa dei propri diritti in un eventuale giudizio; altre finalità, collegate alla principale, possono essere anche richieste dal paziente, come la comunicazione dei dati ad enti privati per finalità assicurative o mutualistiche. Accanto a tali finalità di trattamento, ciascun medico può individuarne altre eventuali che dovranno essere comunque indicate nell'ambito delle informazioni da rendere al paziente. Così se ad esempio il medico tratta i dati per finalità di analisi statistica per fini di ricerca scientifica nel settore sanitario, dovrà renderlo noto nelle informazioni che rende ex art. 13 e chiedere il consenso al trattamento, al pari se tratta i dati personali per inviare ad esempio una newsletter informativa ai pazienti su iniziative organizzate dallo studio, attività redazionale o altro.

Per quanto riguarda invece le modalità di trattamento, dovranno essere indicati i modi attraverso cui i dati sono trattati e conservati, quindi se il trattamento viene effettuato in modalità cartacea e/o elettronica, se vi sono soggetti

(dipendenti/collaboratori) che trattano i dati personali specificando che sono stati istruiti e formati su comportamenti da assumere rispetto ai dati trattati, e che sono abilitati ad accedere solo ai dati necessari per lo svolgimento delle loro mansioni, oltre ad essere tenuti al rispetto degli obblighi di riservatezza. Le informazioni rese al paziente devono evidenziare inoltre in maniera analitica 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: a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente; b) nell'ambito della teleassistenza o telemedicina; c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica; d) ai fini dell'implementazione del fascicolo sanitario elettronico di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dall a legge 17 dicembre 2012, n. 221; e) ai fini dei sistemi di sorveglianza e dei registri di cui all'articolo 12 del decreto - legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.

Nei confronti di un minore le informazioni sono rese ai genitori o a chi esercita la potestà genitoriale, tuttavia, dopo il raggiungimento della maggiore età esse vanno fornite all'interessato nel caso in cui non siano state fornite in precedenza.

Il Consenso è ancora necessario?

Alla domanda, il medico deve chiedere il consenso espresso al trattamento dei dati sanitari per finalità di diagnosi, cura, assistenza sanitaria quando rende le informazioni ex art. 13 del GDPR? Si deve rispondere no. Ai sensi dell'art. 9 lett. h, infatti, non è necessario il 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". Dunque, una volta che il paziente ha scelto di sottoporsi ad una cura o richiesto assistenza sanitaria, non occorre il consenso al trattamento dei suoi dati per tali finalità. Resta il fatto che il regolamento ha lasciato liberi gli Stati di intervenire per disciplinare tale materia con maggiore dettaglio, così il nostro Stato, in linea con quanto stabilito dal Regolamento, ha abrogato la parte del Codice privacy riferita alla richiesta di consenso in materia di trattamento di dati sanitari per finalità di cura e assistenza (art. 81 Prestazione del consenso – abrogato), ma ha stabilito che con cadenza biennale l'autorità di controllo, il Garante Privacy, detti regole deontologiche e misure di garanzia in tale ambito cui i medici dovranno attenersi. Se però il medico intende utilizzare i dati personali del paziente per finalità diverse e ulteriori rispetto a quelle connesse alle prestazioni assistenziali da questi richieste, come ad esempio per sperimentazione

scientifica oppure per inviti ad iniziative dello studio o ancora per inviare newsletter) sono necessari specifici consensi espressi, in relazione ai quali deve essere sempre data la possibilità al paziente di ritirare i permessi manifestati.Resta salvo, ovviamente, il consenso informato necessario alla prestazione sanitaria, che nulla ha a che fare con il consenso al trattamento dei dati personali per finalità di assistenza sanitaria richiesta dal paziente.

Ma se ci si trova in una situazione di urgenza e il paziente è impossibilitato per incapacità fisica, incapacità di agire o di intendere o di volere, a ricevere le informazioni sul trattamento dei dati sanitari o quando non è possibile rendere le informazioni, come si procede?

In tali circostanze particolari, le informazioni di cui agli articoli 13 (o 14 nel caso in cui i dati non siano stati raccolti presso l'interessato, ma siano pervenuti al titolare da altra fonte, ad esempio raccolti dal FSE) del GDPR, ai sensi dell'art. 82 del Codice Privacy modificato, possono essere rese senza ritardo successivamente alla prestazione, a chi esercita legalmente la rappresentanza, o a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi della legge 219/2017 o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato. Ciò si verifica anche nei casi in cui sussista un rischio grave, imminente ed irreparabile perla salute o l'incolumità fisica dell'interessato.Le informazioni possono essere rese anche dopo la prestazione, senza ritardo anche in caso di prestazione medica che può essere pregiudicata dal loro preventivo rilascio, in termini di tempestività o efficacia.

Soggetti autorizzati al trattamento, segretari, infermieri, colleghi collaboratori dello studio medico

Oltre alle informazioni da fornire ai pazienti e all'informativa da rendere a colleghi, collaboratori, dipendenti, fornitori e a tutti gli altri soggetti di cui si trattano eventualmente dati personali, il GDPR richiede al titolare del trattamento di autorizzare i soggetti che nel contesto organizzativo trattano dati personali e in particolare richiede di formarli e istruirli in merito ai comportamenti da adottare nel trattamento dei dati personali. Ciò significa che se nello studio medico vi sono dipendenti, come può essere una segretaria o altri collaboratori ad esempio, colleghi junior, stagisti, infermieri è doveroso che il titolare li istruisca e li autorizzi al trattamento dei dati personali e alle categorie di dati personali. L'autorizzazione può essere effettuata mediante una lettera d'incarico scritta comunicata ad personam, ma non necessariamente, infatti il GDPR, ma anche il nuovo codice concedono al titolare la possibilità di individuare le modalità più adeguate per autorizzare tali soggetti al trattamento dei dati. La cosa importante è che la modalità scelta sia tale da permettere al titolare del trattamento di provare nel caso di ispezione, ma anche nel caso di complicazioni, violazioni, contenziosi in relazione ai dati trattati, che tali soggetti sono stati autorizzati, ma soprattutto formati, istruiti e impegnati alla riservatezza. Senza dimenticare che tali soggetti

dovranno avere dei permessi limitati, circoscritti unicamente a quei dati necessari per permettere loro di svolgere le proprie mansioni; questo significa che ad esempio il/la segretario/a che si occupa solo della parte amministrativa e che gestisce l'agenda del medico, non dovrebbe venire a conoscenza (o avere l'accesso) dei dati sanitari dei pazienti, in quanto non è a ciò abilitata, innanzitutto non essendo un professionista medico e, poi perché tale accesso non risulta necessario ai fini dell'esercizio delle sue funzioni.

Ma quindi la segretaria del medico non può consegnare al paziente la documentazione contenente dati sanitari, né la ricetta medica?

Il personale di segreteria può consegnare al paziente o a chi da lui delegato la documentazione sanitaria o le ricette mediche, ma tali documenti devono essere custoditi in una busta preventivamente sigillata dal medico al quale il paziente ha conferito l'incarico di eseguire una prestazione sanitaria, il personale di segreteria infatti non può entrare nel merito dei dati sanitari del paziente. Quindi, situazioni del tipo: segretaria che per velocizzare prende nota delle richieste dai pazienti, entra nella stanza del medico e riporta le ricette compilate o addirittura riporta brevemente risposte del medico al paziente, mentre la sala d'attesa è gremita di persone, sono da evitare nella maniera più assoluta.E se un paziente delega il figlio a ritirare i documenti contenenti dati sanitari?Un paziente può certamente delegare il figlio o altri a ricevere i documenti contenenti dati sanitari che lo riguardano con apposita delega sottoscritta dal delegante e copia del documento di identità dello stesso. In tal caso, i documenti possono essere consegnati in busta chiusa al delegato.Ma se un datore di lavoro chiede al medico del lavoro da lui incaricato i dati sanitari di un suo dipendente per conferirgli dei permessi speciali?Ciò è ammesso unicamente dietro il consenso espresso del paziente che deve essere scritto, e specifico; è consigliabile trattenere sempre anche copia del documento di identità del paziente, anch'essa firmata.Come comportarsi per gestire correttamente la sala d'attesa? Ad esempio è fondamentale, evitare di lasciare nella sala d'attesa documenti che riportino dati personali o peggio ancora dati sanitari, evitare di inserire armadietti non ben custoditi o lasciati aperti in cui sono conservati dati o informazioni personali o sanitarie; tali armadi dovrebbero essere sempre chusi con cura e posti in una zona diversa dalla sala d'attesa e comunque tenuta sotto controllo; è fondamentale bloccare con password eventuali computer presenti, quando ci si allontana dalla propria postazione. Si tiene a precisare che tali indicazioni, restano accorgimenti di base.

Soggetti autorizzati al trattamento, infermieri, colleghi collaboratori dello studio medico

Eventuali collaboratori medici o personale infermieristico di cui il titolare si avvale nello studio potranno essere autorizzati al trattamento anche dei dati sanitari dei pazienti, di questo va resa nota nelle informazioni rese in sede di raccolta dei dati.Il medico, titolare del trattamento dovrà poi individuare i soggetti esterni cui comunica i dati trattati, si pensi ad esempio al commercialista, a chi

eventualmente gestisce il suo sito internet, che potrebbe accedere a dati personali per finalità di manutenzione del sito, alla società di consulenza che si occupa di effettuare interventi sui sistemi informatici dello studio, alla società che fornisce il gestionale per lo studio o, nel caso ad esempio, di un dentista, all'odontotecnico che fornisce al professionista un supporto una tantum, nel caso di ortopedico al fisioterapista con cui il medico stabilmente collabora. Sebbene, in tali ultimi casi, occorre comunque analizzare in dettaglio il rapporto per comprendere se ci si trova in una situazione di contitolarità del trattamento, titolarità autonoma o rapporto titolare/responsabile. In ogni caso, il rapporto tra professionisti in merito al trattamento dei dati deve essere debitamente contrattualizzato e l'informazione va riportata nell'informativa.

Misure di sicurezza e data breach

Per quanto concerne le misure di sicurezza in merito ai dati personali e sanitari trattati da uno studio medico, il riferimento è l'art. 32 del GDPR che, nel rispetto del principio dell'accountability (responsabilizzazione di chi tratta dati personali), non individua nel dettaglio le misure minime, come diversamente faceva l'abrogato Allegato B del vecchio Codice Privacy, ma offre delle linee guida sulle misure di sicurezza, stabilendo che esse devono essere adottate tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche; si tratta dunque di misure di sicurezza che ciascun titolare e responsabile del trattamento devono individuare in base al modo in cui svolgono il trattamento dei dati, misure di sicurezza che devono essere adatte alla specifica situazione di trattamento al fine di garantire un livello di sicurezza adeguato al rischio. Tali misure devono comprendere, tra le altre, dice l'articolo 32 del GDPR:a. la pseudonimizzazione e la cifratura dei dati personali; b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza si deve tener conto dei rischi che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Quando si parla di data breach si intende una violazione sui dati personali riferita dunque a perdita, modifica, divulgazione illecita o non autorizzata, distruzione, accesso non autorizzato a dati personali. Il GDPR impone ai titolari del trattamento di predisporre una procedura che sia in grado di individuare tempestivamente una violazione sui dati trattati e permettere così di intervenire

immediatamente per evitare che tale violazione possa provocare danni sui diritti e le libertà degli interessati, tale individuazione tempestiva della violazione deve permettere di soddisfare un altro obbligo posto a carico dei titolari del trattamento, quello di comunicare al Garante la violazione subita entro 72 ore decorrenti dal momento in cui il titolare ne ha preso conoscenza, tenendo presente che non tutte le violazioni vanno comunicate al Garante, ma solo quelle potrebbero incidere negativamente sulle persone fisiche, sui loro diritti e sulle loro libertà, provocando danni fisici, morali o immateriali (vanno notificate al Garante dunque solo le violazioni in relazione alle quali il titolare ritenga probabile che dalle stesse derivino rischi per i diritti e le libertà degli interessati); le violazioni che potrebbero provocare danni sui diritti degli interessati devono essere comunicate anche agli stessi.In ogni caso le violazioni di dati personali subite, anche se non notificate all´autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5) devono essere inserite in un registro delle violazioni. La procedura per individuare le violazioni sui dati deve essere predisposta prima che una violazione si verifichi, in modo che nel caso in cui l'evento potenzialmente individuato come rischioso dovesse verificarsi nel concreto, si conoscano già le procedure da eseguire. Occorrerà pertanto anche in tal caso effettuare un'analisi dell'organizzazione per individuare quali azioni meglio si confanno al contesto specifico e indicare a priori eventualmente un soggetto interno cui demandare l'incarico di procedere in tal senso. La procedura deve essere dimostrabile così come l'eventuale incarico attribuito al soggetto che dovrà effettuare le operazioni in caso di data breach, pertanto si consiglia di inserire un capitolo specifico dedicato a tale procedura in un regolamento più ampio da comunicare a tutti coloro che a vari livelli collaborano o lavorano nello studio.

Registro dei trattamenti

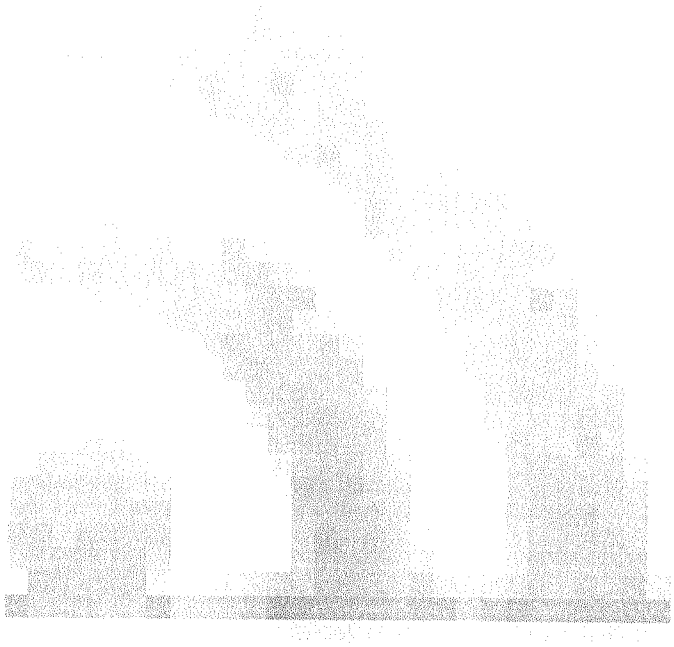
Nel registro dei trattamenti il titolare del trattamento (ma anche il responsabile) deve inserire una serie di informazioni indicate all'art. 30 del GDPR: a. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare 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 (i soggetti terzi cui i dati vengono eventualmente comunicati, ad esempio ASL, Agenzia Entrate, INPS, commercialista, eventualmente cloud service provider), compresi i destinatari di paesi terzi od organizzazioni internazionali; e. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; f. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati (10 anni); g. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui

all'articolo 32, paragrafo 1 o rimandare ad un manuale che le contenga in dettaglio; h. l'indicazione degli assett utilizzati dallo studio; i. la base giuridica del trattamento (assistenza sanitaria, quindi esecuzione contrattuale, obbligo di legge o legittimo interesse del titolare).Il registro dei trattamenti dovrà essere fornito al Garante o all'autorità ispettiva qualora ne facciano richiesta.

Non tutti sono tenuti a redigere il registro, sebbene il Garante ne raccomandi comunque l'adozione, in particolare a chi tratta dati sanitari, come appunto i medici, ritenendo che il registro costituisca in uno strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso. Per facilitare tale onere il Garante ha individuato delle modalità semplificate di tenuta e predisposizione del registro in favore di piccoli studi professionali e PMI, così ha stabilito ad esempio che i piccoli studi medici e le PMI possono circoscrivere la redazione del registro alle sole attività di trattamento riferite alle categorie particolari di dati e/o dati relativi a condanne penali o reati.

Queste sono le operazioni di base che uno studio medico è tenuto ad approntare per approcciarsi in maniera conforme al trattamento dei dati personali trattati, resta inteso che, quanto indicato non deve essere inteso come una consulenza, in quanto ogni contesto organizzativo deve essere analizzato nel dettaglio per consentire di procedere in maniera adeguata nel rispetto del principio di responsabilizzazione.

Un'ultima raccomandazione prima di chiudere: meglio evitare di fornire assistenza medica o informazioni sullo stato di salute di pazienti in chat o peggio ancora in messaggi privati sui social network, se non si tratta di sistemi appositamente ideati e sviluppati per gestire e quindi proteggere anche dati sanitari mediante ad esempio sistemi di crittografia che garantiscono livelli di sicurezza realmente elevati.



(/RSS/Index)

Privacy Policy (https://bdbackofficestorage.blob.core.windows.net/servizi-siteassets/files/Privacy%20Consulenza.pdf)
Termini di Servizio (https://bdbackofficestorage.blob.core.windows.net/servizi-siteassets/files/termini%20di%20servizio_21-11-18.pdf)
Cookie Policy (https://bdbackofficestorage.blob.core.windows.net/servizi-siteassets/files/cookie_consulenza.pdf)