LA PRIVACY NELLO STUDIO MEDICO DOPO IL REGOLAMENTO EUROPEO 679/2016

Ordine dei Medici della provincia di Firenze (Settembre 2018)

-

PREMESSA

I seguenti chiarimenti sono stati redatti tenendo conto delle norme introdotte dal Regolamento Europeo 679/2016, entrato in vigore il 25/05/2018.

Il Decreto Legislativo di adeguamento della normativa italiana a quella europea (D.Lgs. 101/2018) non ha risolto tutte le incertezze interpretative esistenti e ha assegnato all'Autorità Garante per la Privacy il compito di formulare linee guida per semplificare gli oneri a carico delle realtà più limitate. Per cui quanto segue sarà oggetto di periodica revisione e aggiornamento.

Le norme sulla privacy riguardano tutti i medici? Oppure chi non gestisce i dati dei pazienti ne è esonerato?
Prima cosa importante da chiarire: il nuovo Regolamento Europeo (ma era già previsto dalla Legge italiana) definisce "trattamento di dati" ogni operazione di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione di dati, anche se non registrati in una banca di dati, sia che si utilizzi il computer, sia che si lavori su carta.
Sulla base di questa definizione, è praticamente impossibile che il medico non esegua nessun "trattamento" dei dati dei propri pazienti. Ad esempio, anche tenere un'agenda degli appuntamenti con annotati i nominativi dei pazienti è già un trattamento di dati. Anche emettere una fattura con i dati del paziente è un trattamento di dati. Anche fornire le fatture al commercialista per gli adempimenti fiscali è un trattamento di dati.
Per cui si deve concludere che le norme sulla privacy riguardano tutti.

Chiarito questo, cosa deve fare il medico nel suo studio per essere in regola con la privacy dopo l'entrata in vigore del Regolamento Europeo 679/2016?
Ci sono alcuni adempimenti che il medico è tenuto a fare per ottemperare alle norme del Regolamento Europeo, che si possono riassumere così:
- identificare i soggetti interessati al trattamento dei dati;
- predisporre un'adeguata informativa;
- raccogliere il consenso;
- istituire il Registro dei trattamenti dei dati;
- elaborare procedure per fronteggiare le ipotesi di violazione della privacy.

Cominciamo dal primo punto: identificare i soggetti interessati. Chi sono?
Secondo logica, i soggetti interessati al trattamento dei dati da parte di un medico sono i suoi pazienti.
Ma non solo: il medico potrebbe gestire anche i dati personali del suo personale dipendente o dei suoi collaboratori.
Infine il medico potrebbe dover avere necessità di gestire anche i dati personali di soggetti che non sono né suoi pazienti né suoi dipendenti o collaboratori. Ad esempio i fornitori.
Questa ricognizione è il primo passo da fare per calibrare poi i successivi adempimenti.

INFORMATIVA

Cos'è l'informativa sul trattamento dei dati personali?
È una dichiarazione scritta con linguaggio semplice e chiaro da rendere nota al paziente anticipatamente rispetto al trattamento dei dati da redigere in forma concisa, trasparente, intellegibile e facilmente accessibile.
Può essere consegnata ad ogni singolo paziente, oppure può essere affissa nella sala d'attesa dello studio in modo da renderla conoscibile alla generalità degli utenti dello studio.
L'informativa deve contenere tutta una serie di informazioni, secondo quanto previsto dal Regolamento Europeo, che si possono così riassumere:
- dati di contatto del Titolare dello Studio;
- dati di contatto del Responsabile del trattamento dei dati (se presente);
- dati di contatto del Responsabile della protezione dei dati – DPO (se presente);
- finalità e scopo del trattamento dei dati;
- modalità di trattamento dei dati;
- tempo di conservazione dei dati;
- soggetti a cui i dati vengono comunicati;
- trasferimento all'estero dei dati;
- diritti dell'interessato.

E' importante ricordare che l'informativa è un adempimento obbligatorio e in nessun modo eludibile.

Entriamo nel vivo dell'informativa: i dati di contatto
In primo luogo l'informativa deve contenere i dati di contatto del Titolare dello studio (nominativo, sede, telefono, email).
Se il titolare dello studio nomina un responsabile del trattamento dei dati, deve indicare gli stessi dati anche per il responsabile. La nomina di tale responsabile non è obbligatoria.
Se il titolare dello studio nomina un responsabile per la protezione dei dati (DPO), deve indicare gli stessi dati anche per il DPO. Sull'obbligatorietà o meno della figura del DPO si parlerà più avanti.

Finalità e scopi del trattamento
Vanno indicate le finalità del trattamento, cioè lo scopo per cui si raccolgono, si gestiscono e si trattano i dati dei pazienti. La finalità principale per uno studio medico è: *prevenzione, diagnosi, cura, riabilitazione o per altre prestazioni di natura medica o sanitaria richieste dal diretto interessato, anche farmaceutiche o specialistiche*.
Ci sono poi altre finalità, che sono obbligatorie per legge, ad esempio *comunicare i dati a soggetti, enti o autorità a cui la comunicazione sia obbligatoria in forza di disposizioni di legge o ordini delle autorità*.
Oppure le finalità possono derivare da precisi rapporti contrattuali, come ad esempio nel caso di pazienti che aderiscono a fondi mutualistici o a polizze assicurative. In questi casi la finalità dello studio medico è anche quella di *comunicare i dati ad enti privati per motivi assicurativi su richiesta dell'interessato.*
Un'altra importante finalità per cui lo studio medico tratta i dati dei propri pazienti è *esercitare i diritti legali del titolare dello studio, ad esempio il diritto di difesa in giudizio*.
Solitamente questi sono gli scopi e le finalità che ogni studio medico si prefigge nel trattare i dati dei propri pazienti, per cui si può dire che quanto sopra rappresenta l'informativa "minimale" riguardo alle finalità del trattamento. Se il titolare dello studio, avendo riguardo alla sua specifica attività medica, si rende conto che utilizza i dati dei pazienti anche per altri e ulteriori scopi, deve dichiararlo esplicitamente nell'informativa che quindi va adeguatamente integrata.

Quali possono essere queste ulteriori finalità di trattamento?
Ad esempio condurre attività di ricerca scientifica o epidemiologica, utilizzare i dati dei pazienti per pubblicazioni scientifiche o presentazioni ai congressi, spedire una periodica newsletter ai pazienti per informarli sulle attività dello studio.
Sono tutte finalità ulteriori rispetto a quella fondamentale di attività assistenziale che quindi vanno separatamente evidenziate per renderle note al paziente.

Modalità di trattamento dei dati
Il titolare dello studio deve dichiarare che si ispira ai principi di liceità, correttezza, trasparenza, minimizzazione e limitazione dei dati, come previsto dal Regolamento Europeo.
Una formula utilizzabile potrebbe essere la seguente: *I dati potranno essere trattati in forma cartacea ed elettronica, con accesso consentito ai soli operatori autorizzati, precedentemente nominati Responsabili o addetti al trattamento, i quali seguono corsi di formazione specifici e vengono periodicamente aggiornati sulle regole della privacy e sensibilizzati al rispetto e alla tutela della dignità e della riservatezza del paziente. Tutti gli operatori dello Studio che accedono ai dati informatizzati sono identificabili e dotati di password personale; l'accesso ai dati è consentito solo per le finalità legate al ruolo dell'operatore e solo per lo stretto tempo necessario a trattare la prestazione per la quale il paziente si è recato presso lo Studio.*
Lo Studio non svolge attività di profilazione dei dati dei propri assistiti.
All'interno dei locali è vietato, per la riservatezza degli utenti, registrare audio, video e scattare foto.

Tempo di conservazione dei dati
Nell'informativa va anche indicato il tempo di conservazione dei dati da parte dello studio. Si tratta di un termine piuttosto difficile da stabilire a priori e se ne discuterà più approfonditamente in seguito. Intanto una formulazione adeguata nell'informativa potrebbe essere la seguente: *I dati personali e sensibili verranno conservati per il tempo previsto dall'attuale normativa: in particolare, i dati relativi a ciascun episodio assistenziale, raccolti nella relativa scheda sanitaria, verranno conservati a tempo indeterminato, perdurando il rapporto contrattuale di cura.*
Al termine del rapporto contrattuale di cura, lo Studio conserverà i dati per un periodo non superiore al termine prescrizionale di legge per la tutela dei propri diritti legali e di difesa.

Comunicazioni a terzi dei dati
Una formulazione suggerita può essere la seguente: *I dati non verranno in alcun modo diffusi, ma potranno essere trasmessi agli Enti competenti per finalità amministrative o istituzionali, secondo quanto richiesto dalla normativa vigente. Più precisamente, i dati potranno essere comunicati a destinatari appartenenti alle seguenti categorie:*
- soggetti interni allo Studio con funzione di Incaricati al trattamento;
- professionisti medici e personale sanitario, anche con rapporto di collaborazione occasionale con lo Studio;
- soggetti esterni incaricati di funzioni di manutenzione e assistenza dei sistemi informatici e di comunicazione;
- soggetti esterni consulenti in materia fiscale;
- Autorità ed Enti Pubblici competenti per obbligo di legge;
- (eventuali altre categorie di destinatari).
I soggetti appartenenti alle categorie suddette svolgono la funzione di Responsabile del trattamento dei dati, oppure operano in totale autonomia come distinti Titolari del trattamento.
I dati potranno essere comunicati a familiari o conoscenti solo su espressa autorizzazione dell'interessato.

Trasferimento all'estero dei dati
Di norma uno studio medico non ha mai necessità di trasferire all'estero i dati dei propri pazienti. Però bisogna aver presente che lo studio può avvalersi di strumenti informatici che si "appoggiano" su server ubicati al di fuori del territorio italiano.
Per cui una formulazione suggerita può essere la seguente: *I dati personali sono conservati su server ubicati all'interno dell'Unione Europea. Resta in ogni caso inteso che il Titolare, ove si rendesse necessario, avrà facoltà di spostare i server anche extra-UE. In tal caso, il Titolare assicura sin d'ora che il trasferimento dei dati extra-UE avverrà in conformità alle disposizioni di legge applicabili, previa stipula delle clausole contrattuali standard previste dalla Commissione Europea.*

Diritti dell'interessato
In questa sezione dell'informativa occorre riportare i diritti dell'interessato come l'esempio sottostante:
Nella Sua qualità di Interessato, ai sensi dell'art. 15 del GDPR, ha il diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che La riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
a) le finalità del trattamento;
b) le categorie dei dati in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
d) il periodo di conservazione dei dati personali previsto oppure dei criteri determinati per determinare tale periodo;
e) richiedere al Titolare l'accesso ai dati, la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che La riguardano o di opporsi al loro trattamento;
f) con riferimento all'eventuale consenso prestato, il diritto di revocare, in ogni momento, il consenso prestato;
g) il diritto di proporre reclamo all'Autorità Garante;
h) il diritto alla portabilità dei dati.
Devono essere evidenziate le modalità per l'interessato di esercizio dei suoi diritti, ad esempio scrivendo una lettera o una email al titolare dello studio o al responsabile.

Ma se il paziente ha diritto a ottenere "la cancellazione dei suoi dati", come fa il medico a difendersi in caso di contenzioso?
Il diritto alla cancellazione va messo in relazione al diritto del medico di tutelare i suoi interessi legali, per cui se il paziente chiede la cancellazione dei suoi dati prima che siano decorsi i termini di prescrizione legali, il medico può legittimamente rifiutare tale cancellazione, motivando tale decisione con la necessità di tutelare il suo diritto di difesa. Viceversa, se i termini sono oramai decorsi, il medico può tranquillamente procedere alla cancellazione, accogliendo la richiesta del paziente.
In altre parole, il "diritto all'oblio" non è assoluto: trova un limite nel diritto del medico a tutelare i suoi diritti legali.

E cosa significa che il paziente può "revocare il consenso"? Senza di quello non può più essere curato….
Esatto. Se il paziente revoca il suo consenso al trattamento dei dati per le finalità di prevenzione, diagnosi e cura, il medico non può più legittimamente averlo in cura. Per cui, fermo restando il principio di tutela in casi di emergenza, il rapporto assistenziale è da intendersi terminato.

Cosa significa la "portabilità dei dati"?
Significa che il paziente ha diritto ad ottenere i dati che lo riguardano in un formato facilmente accessibile e gestibile con sistemi informatici.

Quindi il paziente ha diritto a chiedere che lo studio medico gli fornisca i suoi dati o in forma cartacea o in forma digitale (in un formato facilmente accessibile).
Se il paziente lo richiede, lo studio deve essere in grado di trasmettere i dati ad un altro studio medico indicato dal paziente stesso. E anche in questo caso il formato di trasmissione deve assicurare la facilità di accesso e di interscambio.

CONSENSO

Una volta che il paziente è stato informato, cosa deve fare il medico?
Deve raccogliere il consenso.
Il consenso può essere raccolto anche in forma orale, ma per evitare future ed eventuali contestazioni è opportuno che venga raccolto in forma scritta, con la sottoscrizione di un apposito modulo, anche redatto in calce all'informativa.
Se lo studio intende utilizzare i dati per finalità diverse e ulteriori rispetto a quelle meramente assistenziali (ad esempio: per sperimentazione scientifica oppure per pubblicare i dati del paziente su riviste medico-scientifiche o presentazioni a congressi oppure per inviare newsletter periodiche informative) sono necessari ulteriori e differenziati consensi.

Questo consenso firmato dal paziente è "una tantum" o va rinnovato periodicamente?
Il consenso del paziente resta valido a tempo indeterminato.

Chi può esprimere il consenso? Solo il diretto interessato?
Generalmente sì. Il paziente maggiorenne, capace di intendere e di volere, è l'unico soggetto autorizzato a dare il consenso per il trattamento dei propri dati sanitari.
Se il paziente invece è minorenne o non è capace di intendere e di volere, allora il consenso deve essere dato rispettivamente dai genitori (anche disgiuntamente) o da chi esercita la potestà genitoriale o dal tutore.

A proposito dei minorenni: c'è qualche differenza se i genitori sono sposati o separati o divorziati?
No, nessuna differenza.
Entrambi i genitori, indipendentemente dal loro status giuridico, hanno il dovere di tutelare la salute dei propri figli, per cui hanno il diritto-dovere di essere informati sullo stato di salute dei figli e il medico deve portare a loro conoscenza i dati sanitari di cui dispone, o disgiuntamente o congiuntamente. È responsabilità dei genitori (e non del medico) relazionarsi fra loro.

Il consenso di cui stiamo parlando equivale al consenso al trattamento sanitario?
Assolutamente no.
Il consenso di cui stiamo parlando riguarda esclusivamente l'autorizzazione che il paziente dà al medico al trattamento dei dati ai fini della privacy.
Tutt'altra cosa è il consenso del paziente all'atto medico, che non riguarda la legge sulla privacy, bensì l'art. 32 della Costituzione, a norma del quale nessuno può essere obbligato ad un trattamento sanitario contro la sua volontà.
Adesso ci stiamo occupando solo e soltanto del consenso ai fini della legge sulla privacy.

E se il consenso viene revocato?
Come già detto sopra, se il paziente revoca il suo consenso al trattamento dei dati per finalità di prevenzione, diagnosi e cura, il rapporto assistenziale non può proseguire e quindi è da ritenersi concluso (fatte salve le situazioni di emergenza).

Se invece il paziente revoca il consenso per finalità diverse (ad esempio, non vuole più ricevere le newsletter dallo studio), il rapporto assistenziale prosegue normalmente e si interrompe solo il trattamento dei dati per la specifica finalità per la quale il consenso è stato revocato.

FORMALIZZAZIONE DEI RUOLI

Oltre a riformulare l'informativa e raccogliere il consenso, cos'altro deve fare il medico nel suo studio?
Se il medico, nel proprio studio, si avvale di personale di segreteria, deve redigere una formale lettera al personale di segreteria, che si deve attenere alle istruzioni impartite dal medico titolare dello studio. Un modello di lettera di incarico può essere il seguente:

Il sottoscritto/a …….....…… in qualità di Titolare del trattamento dei dati dello Studio medico …….…….. con sede in …….

NOMINA QUALE ADDETTO AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI

il signor/a …… nato/a a …… il ……

In particolare dovrà:

a) raccogliere, registrare, trattare e conservare i dati personali e sensibili contenuti nelle cartelle cliniche, sia su supporto cartaceo che informatico, avendo cura che l'accesso agli stessi sia consentito solo ai soggetti autorizzati;

b) adempiere alla comunicazione dei dati ai soggetti esterni nelle forme previste.

Le rammento che dovrà adottare la parola chiave riservata per l'accesso alla banca dati elettronica che dovrà essere periodicamente modificata.

Data ……

FIRMA DEL TITOLARE

per ricevuta: Firma dell'Incaricato

Si consiglia di allegare la copia del documento di identità dell'addetto.

Se il medico si avvale di collaboratori medici o personale infermieristico?
Se il medico, nel proprio studio, si avvale di collaboratori medici o personale infermieristico, deve redigere una formale lettera a tali soggetti conferendogli apposita responsabilità alla tutela della privacy. Un modello di lettera può essere il seguente:

Il sottoscritto/a …….....…… in qualità di Titolare del trattamento dei dati dello Studio medico …….…….. con sede in …….

NOMINA QUALE RESPONSABILE AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI

il signor/a …… nato/a a …… il ……

In particolare dovrà:

a) raccogliere, registrare, trattare e conservare i dati personali e sensibili contenuti nelle cartelle cliniche, sia su supporto cartaceo che informatico, avendo cura che l'accesso agli stessi sia consentito solo ai soggetti autorizzati;

b) adempiere alla comunicazione dei dati ai soggetti esterni nelle forme previste.

Le rammento che dovrà adottare la parola chiave riservata per l'accesso alla banca dati elettronica che dovrà essere periodicamente modificata.

Data ……

FIRMA DEL TITOLARE

per ricevuta: Firma dell'Incaricato

Si consiglia di allegare la copia del documento di identità del collaboratore.

Se il medico si avvale di un ragioniere e/o commercialista per la tenuta della sua contabilità?
Anche in questo caso va affidata al commercialista la formale responsabilità per il trattamento dei dati. Si può utilizzare il seguente modello di lettera:

Il sottoscritto/a …….....…… in qualità di titolare del trattamento dei dati dello Studio medico/Studio medico associato …….…….. con sede in …….

NOMINA QUALE RESPONSABILE AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI

Il/la signor/a - Il/La dott./ssa titolare di Studio commercialista con sede in…… nato/a a …… il …….....

In particolare dovrà:

a) raccogliere, registrare, trattare e conservare i dati personali e sensibili sia su supporto cartaceo che informatico, avendo cura che l'accesso agli stessi sia consentito solo ai soggetti autorizzati;

b) adempiere alla comunicazione dei dati ai soggetti esterni nelle forme previste.

Le rammento che dovrà adottare la parola chiave riservata per l'accesso alla banca dati elettronica che dovrà essere periodicamente modificata.

Data ……

FIRMA DEL TITOLARE

per ricevuta: Firma del Responsabile

Si consiglia di allegare la copia del documento di identità del commercialista.

E nel caso dell'odontoiatra che si avvale dell'opera dell'odontotecnico?
Anche in questo caso è necessario che l'odontoiatra rediga una apposita lettera per affidare la responsabilità per il trattamento dei dati:

Il sottoscritto/a …….....…… in qualità di titolare del trattamento dei dati dello Studio odontoiatrico/ Studio odontoiatrico associato …….…….. con sede in …….

NOMINA QUALE RESPONSABILE AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI

il signor/a …… nato/a a …… il …..... , Titolare del Laboratorio odontotecnico con sede……

In particolare dovrà:

a) raccogliere, registrare, trattare e conservare i dati personali e sensibili contenuti nelle cartelle cliniche, sia su supporto cartaceo che informatico, avendo cura che l'accesso agli stessi sia consentito solo ai soggetti autorizzati;

b) adempiere alla comunicazione dei dati ai soggetti esterni nelle forme previste.

Le rammento che dovrà adottare la parola chiave riservata per l'accesso alla banca dati elettronica che dovrà essere periodicamente modificata.

Data ……

FIRMA DEL TITOLARE

per ricevuta: Firma del Responsabile

Si consiglia di allegare la copia del documento di identità dell'odontotecnico.

E se lo studio è composto da più medici in forma associativa?
Se i dati dei pazienti sono condivisi da più medici in forma stabile e continuativa, fermo restando che ciascun medico è titolare dei dati dei suoi diretti assistiti, può essere necessario sottoscrivere un accordo di contitolarità per legittimare il trattamento in comune dei dati.
Ovviamente si tratta di una situazione che va esplicitata nell'informativa e che renderà necessario approntare misure di sicurezza adeguate.

REGISTRO DEI TRATTAMENTI

Oltre a tutto questo bisogna preoccuparsi del "Registro dei Trattamenti". Cos'è in pratica?
E' un registro in cui si elencano le tipologie di trattamenti che vengono svolti dallo studio e che coinvolgono i dati personali degli interessati.
Può essere composto come un semplice foglio in formato Excel (ce ne sono molti esempi su internet) oppure può essere realizzato dall'azienda informatica che fornisce il software gestionale dello studio.

In che cosa consiste?
Si tratta di un documento tenuto in forma libera e conservato dove il professionista svolge l'attività.
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.

E' obbligatorio per tutti gli studi medici?
Siccome gli studi medici trattano dati inerenti la salute dei propri assistiti, che sono dati particolarmente delicati e sensibili, al di là dell'esistenza di uno specifico obbligo è fortemente raccomandato approntare il registro, come previsto dall'art. 30 del Regolamento Europeo.
Infatti può rappresentare uno strumento utile per dimostrare a chiunque che lo studio è particolarmente attento alla riservatezza dei dati dei suoi clienti-pazienti, a beneficio della sua attività.

Cosa deve essere riportato sul registro?
In tale Registro devono essere annotati:
- identificativi del titolare dello studio e del responsabile (se presente);
- la denominazione del trattamento (ad esempio: gestione sanitaria dei pazienti);
- la finalità del trattamento (ad esempio: rapporto di cura);
- la tipologia del trattamento (ad esempio: normale);
- le categorie di soggetti interessati (ad esempio: pazienti);
- le categorie di dati personali trattati (ad esempio: dati relativi alla salute);
- le categorie di destinatari a cui i dati possono o devono essere comunicati (ad esempio: ASL, INPS, INAIL, Agenzia delle Entrate, Autorità Giudiziaria, Compagnie Assicurative, ecc.);
- gli eventuali responsabili esterni (ad esempio: il commercialista o il consulente del lavoro);
- i Paesi stranieri verso cui i dati possono essere trasferiti (ad esempio: nessuno);
- le garanzie adottate per il trasferimento internazionale di dati (ad esempio: nessuna);
- il periodo di conservazione dei dati (ad esempio: 10 anni o comunque per il tempo necessario a tutelare i diritti legali del titolare);
- il software informatico utilizzato per il trattamento dei dati;
- le misure di sicurezza fisiche, organizzative ed informatiche adottate per la protezione dei dati;
- la base giuridica su cui si fonda il trattamento (ad esempio: obbligo legale oppure consenso dell'interessato);
- la fonte dei dati personali (ad esempio: conferiti dall'interessato o acquisiti dal suo FSE);
- la necessità o meno di una valutazione d'impatto sulla protezione dei dati.

Il registro dei trattamenti è uno soltanto?
Dipende dall'organizzazione dello studio medico.
Nello studio monoprofessionale è sufficiente la predisposizione di un solo registro dei trattamenti a cura del titolare dello studio.
In altri contesti operativi potrebbe essere necessaria la predisposizione di un registro dei trattamenti per il titolare e uno per il responsabile del trattamento dei dati.

POLITICHE DI SICUREZZA

Dopo aver scritto l'informativa, fatto firmare i consensi e compilato il Registro dei trattamenti sono finiti gli adempimenti?
Da questo momento in poi scatta la parte "sicurezza dei dati" nel senso che gli adempimenti che sono stati illustrati fino ad ora non esauriscono, ma anzi avviano un processo di protezione e tutela nel trattamento dei dati perché, secondo il Regolamento Europeo, chi gestisce i dati deve agire sul principio della "responsabilizzazione", cioè sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione delle norme di tutela e protezione della privacy.
Ad esempio, fin dall'inizio bisogna configurare il trattamento dei dati prevedendo le garanzie indispensabili per soddisfare i requisiti del Regolamento Europeo e tutelare i diritti degli interessati. A questo proposito, i

produttori di software informatico gestionale per gli studi medici sono tenuti a ripensare i loro prodotti preoccupandosi della tutela della privacy fin dalla progettazione del software che dev'essere conforme al Regolamento Europeo "by default".
Allo stesso modo il medico nel suo studio deve orientare la propria organizzazione di lavoro in modo sempre assolutamente attento alla tutela della riservatezza dei dati dei pazienti fin dall'origine, evitando comportamenti o prassi che mettano a rischio i diritti e le libertà personali degli interessati.
Ad esempio, 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 questo deve avvenire costantemente e deve sostanziarsi in una serie di attività specifiche e dimostrabili, con monitoraggi periodici.

Ho sentito parlare di "Data Breach". Cosa significa?
Il termine indica ogni "violazione dei dati" e nella pratica può significare ad esempio il furto, la perdita, l'alterazione, la manipolazione di dati cartacei o informatici.
In questi casi il titolare dello studio deve notificare il fatto all'Autorità Garante per la privacy entro 72 ore dal momento in cui ne è venuto a conoscenza. Ma non basta notificare il fatto che si è subita una violazione: bisogna anche dire cosa si è fatto per contenere il danno.
Siccome queste eventualità non sono purtroppo rare, è assolutamente indispensabile che il titolare dello studio progetti e rediga una "procedura di emergenza" con la quale fronteggiare simili evenienze. Tale procedura di emergenza deve essere approntata prima che si verifichino fenomeni di violazione, proprio per essere in grado, prima possibile, di farvi fronte nel modo tecnicamente e organizzativamente più adeguato.
Un po' come quando si sale in aereo: le procedure di emergenza vanno elaborate e rese note prima che l'aereo stia precipitando…

In concreto, qual è la procedura di emergenza da seguire?
Dipende dall'organizzazione dello studio.
Ad esempio il titolare dello studio potrebbe stabilire a priori che, in caso di violazione di dati, lui personalmente o un suo incaricato appositamente individuato, svolga alcune operazioni essenziali e basilari come ad esempio: spengere il server; spostarlo in un luogo più sicuro; interrompere l'energia elettrica; spostare i fascicoli in un luogo più sicuro; allertare i Vigili del Fuoco, ecc.
Bisogna prevedere gli interventi di emergenza ritenuti più adeguati al caso concreto, metterli per iscritto e seguirli in caso di "data breach".

Quali accorgimenti deve adottare il medico che non utilizza il computer, ma conserva tutto su carta?
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. 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. Inoltre l'armadio dovrebbe essere di materiale ignifugo, in modo da evitare il rischio di perdita o distruzione di dati a causa di incendio.

E se il medico utilizza anche il computer?
Vale lo stesso principio di evitare o ridurre al minimo il rischio di perdita, distruzione, sottrazione,

manomissione o alterazione dei dati memorizzati nel computer.
Ciò si può realizzare con diversi accorgimenti tecnici. In primo luogo il computer deve essere protetto da una password alfanumerica (la meno intuitiva possibile) che deve essere cambiata ogni tre mesi. Inoltre il computer deve essere protetto da un software antivirus, anti-malware e, se è connesso a internet, anche da un firewall di ultima generazione, capace di identificare le minacce e bloccarle prima che si concretizzino. Infine deve essere previsto un salvataggio periodico dei dati da poter utilizzare in caso di emergenza.
Le misure di protezione informatica hanno una rapida evoluzione tecnologica, per cui è assolutamente necessario che il medico possa contare su un consulente informatico di propria fiducia per rendere il suo sistema sempre protetto al massimo grado.

Il sostituto o comunque il collaboratore medico può usare il computer del medico titolare?
Allo stesso modo con cui il sostituto o il collaboratore medico può accedere ai fascicoli cartacei dei pazienti, può certamente accedere ai dati sanitari memorizzati nel computer dello studio.
Però è necessario che vi acceda con un proprio nome utente e una propria password, in modo che sul computer rimanga una "traccia informatica" di chi, come e quando ha acceduto al sistema.
Come già detto sopra, a monte ci deve essere una formale lettera di attribuzione di responsabilità.

E il personale di segreteria? Può accedere al computer e alle schede dei pazienti?
Il personale di segreteria deve limitare l'accesso solo ai dati necessari per svolgere il proprio lavoro, per cui potrà sicuramente accedere ai dati personali dei pazienti come ad esempio l'indirizzo e il numero di telefono, ma non ha titolo per accedere ai dati sanitari dei pazienti.
Anche in questo caso è necessario che l'accesso al computer sia effettuato con un nome utente e una password dedicata al personale di segreteria, in modo che il sistema limiti automaticamente l'accesso ai dati comuni e non a quelli sensibili.
E anche in questo caso, come già detto, a monte ci deve essere una formale lettera di attribuzione dell'incarico.

Ma il "Documento Programmatico per la sicurezza" (DPS) esiste sempre?
Il DPS deve ritenersi superato dal Regolamento Europeo che non parla più di "misure minime di sicurezza", ma obbliga il titolare a pensare alla sicurezza al massimo grado.
In pratica col Regolamento Europeo non bisogna limitarsi ad adottare misure di sicurezza minime, ma all'opposto bisogna approntare le procedure che diano il massimo di garanzie tecnicamente possibili per tutelare e proteggere i dati.
Ed in effetti: costruire per bene l'informativa, redigere correttamente il Registro dei Trattamenti e monitorare costantemente le proprie procedure per evitare i rischi di Data Breach sono tutte azioni che rientrano nell'ottica della tutela della riservatezza "al massimo grado" possibile, sia in termini di sicurezza fisica (luoghi e ambienti) che organizzativa (procedure e incarichi) che informatica (strumenti hardware e software adeguati).

Il medico deve segnalare a qualche autorità il fatto che possiede una banca dati (cartacea o su computer) di dati di pazienti?
No, non ha alcun obbligo di segnalare il possesso di una banca dati.
L'unico obbligo di segnalazione è il DPO se nominato (vedasi poi).

In definitiva, è preferibile usare il cartaceo o il computer?
E' una scelta che dipende esclusivamente dalle modalità organizzative del singolo medico. Nessuno dei due sistemi è migliore dell'altro. Semplicemente se si lavora solo su carta, dovranno essere adottati alcuni

accorgimenti; se si lavora col computer, altri. Si può solo dire che nella fase attuale di progresso tecnologico, l'uso del computer è sempre più utile e semplifica notevolmente il lavoro, purché ovviamente venga utilizzato con criterio e diligenza.

IL DPO

Parliamo adesso del DPO: chi è?
Il Regolamento Europeo ha introdotto la figura del "Responsabile della Protezione dei Dati" (in italiano RPD e in inglese DPO).
Si tratta di un soggetto, persona fisica o giuridica, nominato dal titolare con il compito di collaborare con lui nella protezione dei dati e che quindi può affiancare il titolare anche nella redazione dell'informativa, nella gestione del Registro dei Trattamenti, nell'elaborazione delle procedure di emergenza e nel monitoraggio costante e continuativo delle prassi all'interno dello studio.
Il DPO funge anche da punto di contatto con l'Autorità Garante per la Privacy ed è per questo motivo che il suo nominativo va comunicato al Garante.

Lo studio medico è obbligato a nominare un DPO?
La questione non è ad oggi chiaramente risolta, tant'è che la Federazione Nazionale degli Ordini dei Medici ha chiesto un approfondimento al Garante per la Privacy proprio per chiarire l'obbligatorietà o meno di tale nomina.
Nel frattempo i vari esperti di privacy ritengono che la nomina possa essere evitata da parte degli studi medici monoprofessionali (cioè con un solo medico) mentre sarebbe consigliata agli studi medici in cui collaborano stabilmente due o più professionisti.
Ma al momento non è possibile essere più precisi.

Come si fa ad individuare il DPO giusto?
Il Regolamento Europeo non prevede specifici requisiti per svolgere la funzione di DPO. E' però necessario che sia un soggetto esperto in materia di privacy 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.
Ad esempio, lo studio medico che tratta i dati dei pazienti tramite un software adeguato alle normative privacy, potrebbe nominare come DPO la stessa azienda informatica fornitrice del software.

Studi medici autonomi possono nominare lo stesso DPO?
Certamente.
Il DPO è un professionista o un'azienda che lavora con più clienti, per cui lo stesso DPO può svolgere tale servizio per più studi medici contemporaneamente.

SUGGERIMENTI PRATICI

Il paziente ha diritto di chiedere al medico solo una copia degli atti o può pretendere di ottenere gli originali?
Come già detto sopra, il paziente ha diritto alla "portabilità dei dati".
Questo non significa che il medico si deve necessariamente privare dei dati per darli al paziente. Bisogna

distinguere: se il paziente a suo tempo ha consegnato al medico un documento sanitario (ad esempio una radiografia) e poi successivamente chiede che gli venga restituita, il medico deve consegnare lo stesso originale che aveva ricevuto dal paziente stesso (facendosi firmare una ricevuta di consegna). Se invece il paziente chiede la propria scheda sanitaria, può ottenerne una stampa o una fotocopia o in formato digitale facilmente accessibile.

E se la richiesta proviene da un familiare o da un conoscente del paziente?
Dipende se il paziente ha dato il suo consenso. Se è così, allora il medico è autorizzato a fornire i dati sanitari ai familiari o conoscenti individuati dal paziente stesso. Ma se non è così il medico non può rivelare alcunché a nessun soggetto diverso dal diretto interessato.
Per evitare contestazioni, è opportuno che il medico si faccia indicare per iscritto chi sono i soggetti a cui acconsente che siano forniti dati e/o informazioni sul suo stato di salute.

La consegna di documenti sanitari (ad esempio un certificato medico o una ricetta) deve farla materialmente il medico o può farlo anche il personale di segreteria?
Può farlo anche il personale di segreteria, ma in tal caso il documento sanitario deve sempre essere chiuso in una busta e spetterà al personale di segreteria identificare il soggetto che ritira la busta: se il diretto interessato o se un delegato. In quest'ultima ipotesi, dovrà acquisire la delega del diretto interessato.

La delega al familiare o al conoscente deve essere rinnovata volta per volta?
Il paziente può liberamente decidere di dare una delega ad hoc per il ritiro di un singolo documento che lo riguarda, oppure può autorizzare il medico in via continuativa a fornire i dati e i documenti al proprio delegato, senza scadenza.
Il medico si deve attenere a quanto ha indicato il paziente.

Le buste chiuse contenenti i documenti sanitari possono essere messe a disposizione dei pazienti per il ritiro, ad esempio in uno scaffale della sala d'attesa dello studio?
No, perché così facendo non si sa chi è il soggetto che ritira la busta e potrebbe anche succedere che il paziente (magari anche in buona fede) ritiri una busta che non è la sua.
Per evitare questi rischi di indebita conoscenza di dati sanitari da parte di terzi non autorizzati, una efficace misura di sicurezza, ad esempio, è inserire le buste in appositi schedari ubicati non nella sala d'attesa dello studio, bensì nello spazio dedicato alla segreteria. In questo modo l'identificazione del soggetto e la consegna della busta è mediata dal personale di segreteria, che deve attenersi alle regole di tutela della privacy sopra descritte.

Se il paziente chiede al medico una attestazione dettagliata del suo stato di salute, perché per esempio deve presentarla al datore di lavoro per usufruire di permessi speciali, o alla compagnia di assicurazione per un risarcimento, il medico può rifiutarsi di farlo per motivi di privacy?
Assolutamente no.
La decisione se rivelare al datore di lavoro o ad altri soggetti i dati inerenti lo stato di salute spetta al paziente, non al medico. Quindi se il paziente desidera ottenere dei permessi speciali o benefici assicurativi e vuole giustificare questa richiesta con una certificazione medica dettagliata, il medico deve soddisfare la richiesta del suo assistito, dichiarando i dati sanitari in suo possesso (ovviamente secondo verità). Non è compito del medico sindacare questa decisione del paziente.

E se la richiesta di dati e informazioni sanitarie proviene da un qualunque altro soggetto?
In generale vale la regola per cui senza il consenso del diretto interessato, il medico non può comunicare niente a nessuno.

Quindi, solo se c'è il consenso del paziente il medico può fornire dati e informazioni sanitarie ad altri soggetti, come ad esempio alla compagnia di assicurazione del paziente, al datore di lavoro del paziente, e così via.

Ci sono casi in cui il medico è autorizzato a comunicare a terzi i dati sanitari del paziente, in assenza del suo consenso?
Sì, ma sono previsti da specifiche norme di legge (nazionali o regionali) e ciò deve già risultare dall'informativa, come detto sopra.
Per esempio nei casi in cui sussiste obbligo di referto, il medico è tenuto a segnalare all'autorità giudiziaria i dati in suo possesso anche senza il consenso del diretto interessato. Oppure per la segnalazione di malattie infettive o diffusive.
Così come i medici convenzionati (medici di famiglia e pediatri) sono tenuti a comunicare i dati degli assistiti alla ASL per motivi di controllo della spesa sanitaria.

Al di fuori di questi casi, esistono altre situazioni in cui il medico può derogare all'obbligo della riservatezza?
Sì, in ipotesi particolari in cui si renda necessario tutelare la salute di un terzo o della collettività, oppure di un minore, di un soggetto disabile o comunque di un soggetto in situazione di particolare fragilità.

Si può fare qualche esempio di queste situazioni particolari?
Per esempio, se il medico ha in cura un paziente psichiatrico e vi è il rischio concreto e attuale che costui possa costituire un pericolo per l'incolumità di terzi o della collettività, deve segnalare il caso alle competenti autorità (servizi sociali e/o autorità giudiziaria).
Oppure se il medico ha in cura un minore e constata che è oggetto di maltrattamenti o abusi, deve segnalare il caso alle medesime autorità.
Si tratta di situazioni molto delicate, nelle quali il medico deve agire con la massima prudenza e attenzione, valutando caso per caso. Ma ricordando che il diritto alla privacy del paziente può essere superato se sussistono ragioni in cui prevale la necessità di tutelare interessi più rilevanti.

E come si deve comportare il medico a cui l'autorità giudiziaria chiede di rendere testimonianza o di esibire documenti riguardanti un suo paziente?
Il medico può sempre opporre il segreto professionale e rifiutarsi di rendere testimonianza o di esibire documenti.
In questi casi spetta al magistrato valutare se la testimonianza del medico è indispensabile per la soluzione della vertenza giudiziaria o meno. In tal caso il magistrato può decidere che il segreto debba cedere alle superiori esigenze di giustizia e quindi ordinare al medico di deporre. In questi casi il medico non può più rifiutarsi e al contempo è liberato dall'obbligo del segreto, proprio perché vi è un ordine del giudice.

Il diritto alla privacy esiste anche per il paziente defunto?
Le norme del Regolamento Europeo non si applicano alle persone decedute.
Bisogna però ricordare che gli eredi del defunto subentrano in tutti i diritti del deceduto, per cui nei confronti di costoro il medico non può opporre il segreto.
Se, per esempio, il paziente aveva una polizza assicurativa sulla vita, una volta deceduto i dati sanitari di costui possono essere comunicati agli eredi e anche alla compagnia di assicurazione, visto che nel contratto assicurativo il paziente aveva autorizzato la compagnia ad accedere a tali atti al momento della sua morte.

Per quanto tempo il medico deve conservare i dati dei pazienti nel proprio studio?
Oltre quanto già accennato sopra, si può aggiungere che per gli studi medici privati, a differenza degli

ospedali e delle case di cura, non esiste una norma di legge specifica che stabilisca la durata di conservazione degli atti sanitari.
Vale la regola generale secondo cui i dati vanno conservati per il tempo necessario al perseguimento della finalità per cui sono stati raccolti. Tradotto nella prassi medica, significa che il medico deve conservare gli atti fin tanto che dura il rapporto di cura.
Tuttavia bisogna ricordare che a norma del Codice Civile, i documenti amministrativi di un lavoratore autonomo devono essere conservati per almeno 10 anni.
Per cui, in conclusione, il comportamento corretto del medico consiste nel conservare gli atti dei pazienti per tutta la durata del rapporto di cura e per almeno i 10 anni successivi al termine di esso.

Il medico che cessa la propria attività come deve comportarsi?
Vale quanto detto sopra: la cessazione dell'attività corrisponde alla cessazione del rapporto di cura.

La conservazione degli atti per tutti questi anni può non essere agevole…
E' vero, però bisogna tener conto che potrebbero (anche solo come ipotesi teorica) insorgere contestazioni, vertenze o cause fra medico e paziente e se il medico non dispone più della documentazione clinica non ha nemmeno strumenti per dimostrare la correttezza del suo operato. Conservare i documenti, quindi, significa anche conservare le prove della propria correttezza professionale.

Il medico, nel proprio studio, deve predisporre "distanze di cortesia" o sistemi di chiamata numerica?
A differenza delle strutture sanitarie pubbliche o private, che sono locali aperti al pubblico e dove è obbligatorio adottare misure per la riservatezza dei pazienti, negli studi medici privati, che non sono locali aperti al pubblico, non è obbligatorio adottare simili accorgimenti.
Tuttavia il medico (e il personale del suo studio) deve comunque rispettare la riservatezza dei pazienti, per cui vanno evitati tutti i comportamenti che possano essere poco rispettosi della privacy di ognuno. Sta al medico individuare, nel concreto, le modalità più idonee.

A telefono il medico può divulgare dati sanitari dei pazienti? Per esempio comunicare l'esistenza di una certa patologia?
Per i colloqui telefonici vale la stessa regola prevista per i colloqui di persona.
Quindi al diretto interessato si può comunicare ogni informazione sanitaria, sia di persona che per telefono.
Ai soggetti terzi, anche se familiari, la comunicazione (di persona o per telefono) è possibile solo con il consenso del diretto interessato.

E si può usare Whatsapp o strumenti simili nel rapporto medico-paziente?
Gli strumenti di chat o messaggistica non danno alcuna garanzia legale sull'identità del mittente.
Detto in altre parole, mentre al telefono si ha la ragionevole possibilità di identificare colui che sta dall'altra parte della cornetta perché se ne conosce la voce, nelle chat o nei messaggi non c'è modo per avere una minima sicurezza su chi c'è dall'altra parte.
Si tratta di strumenti certamente molto utili nelle relazioni quotidiane, ma probabilmente non sono il mezzo migliore per comunicare e trasmettere dati sensibili come quelli inerenti la salute.

Al paziente bisogna dire sempre tutto riguardo al suo stato di salute, o è meglio essere generici?
Il paziente ha diritto di sapere tutto sul suo stato di salute, senza nessun limite.
Ovviamente, siccome il medico non è un burocrate, ma un professionista, deve aver cura di fornire le informazioni, soprattutto quando riguardano patologie serie, nel modo più consono ed appropriato, tenendo conto della personalità del paziente e rispettando la sua sensibilità.
In proposito vale il principio sancito dal Codice Deontologico: le informazioni riguardanti prognosi gravi o

infauste o tali da poter procurare preoccupazione e sofferenza alla persona, devono essere fornite con prudenza, usando terminologie non traumatizzanti e senza escludere elementi di speranza. La documentata volontà della persona assistita di non essere informata o di delegare ad altro soggetto l'informazione deve essere rispettata.

Veniamo ora ai documenti che contengono dati sanitari. Per esempio, i certificati di malattia devono riportare la diagnosi?
I certificati di malattia per pazienti che sono lavoratori dipendenti devono essere redatti prioritariamente con la procedura telematica, nella quale è previsto che l'indicazione della diagnosi sia portata a conoscenza solo dell'INPS ma non del datore di lavoro.
Ma anche per i certificati cartacei vale la stessa regola, e cioè che la diagnosi non deve essere portata a conoscenza del datore di lavoro.
Fanno eccezione solo i lavoratori dipendenti delle Forze Armate, della Polizia di Stato e dei Vigili del Fuoco, perché in questi casi il datore di lavoro deve per legge essere a conoscenza del tipo di patologia sofferta dal militare. Ecco perché nei confronti di questi pazienti è tutt'ora obbligatorio il certificato cartaceo e non quello telematico.

E per i bambini che frequentano la scuola?
In caso di malattie infettive o diffusive, il medico è tenuto alla segnalazione, che però deve essere fatta alla ASL e non alla scuola.
La scuola, quindi, non può pretendere alcun certificato di malattia dell'alunno, ma semmai solo un certificato per la riammissione a scuola, una volta superata la malattia.
È evidente, quindi, che in questi casi il medico non deve mai indicare alcuna diagnosi nel certificato.

E per i pazienti che non sono né lavoratori dipendenti né studenti?
Allora si tratta di certificati di malattia che il paziente chiede per suoi motivi privati. In questi casi deve essere lo stesso paziente a chiedere al medico se indicare o meno la diagnosi sul certificato, tenendo conto dell'uso che egli ne vorrà fare.

Oltre ai certificati, ci sono molti altri tipi di documenti che contengono dati sanitari di pazienti….
E' proprio così. Nella pratica medica i documenti possono assumere moltissime forme: si pensi ai documenti cartacei come le ricette, i certificati, le cartelle cliniche, le perizie, le relazioni e così via. Come sono altrettanti "documenti" anche i cd o le lastre della diagnostica per immagini.
Quello che è importante ricordare è che la tutela della legge riguarda i "dati sanitari" indipendentemente del "supporto" che li ospita. Ma siccome il medico è tenuto a tutelare e proteggere la riservatezza dei dati sanitari, è evidente che i supporti che li contengono devono avere un adeguato sistema di protezione.

C'è un consiglio "finale" che, in conclusione, può essere dato ai medici?
Come già detto in precedenza, i medici sono i professionisti che più di tutti, per tradizione millenaria, hanno nel loro patrimonio etico e deontologico la tutela del segreto professionale e della riservatezza dei pazienti che hanno in cura.
Questo valore deve essere mantenuto vivo e operante perché è alla base del rapporto fiduciario, in quanto nessun paziente riporrebbe la sua fiducia in un medico che divulgasse sconsideratamente e a chiunque le informazioni che ha acquisito.
Proseguendo, quindi, in questo "binario" etico e deontologico, il medico troverà sempre il modo per affrontare le varie e disparate situazioni in cui si trova ad operare, fondando il suo agire sulla propria coscienza, sensibilità e accortezza.