Il trattamento dei dati sanitari da parte degli esercenti la professione di ostetrica in regime di libera professione alla luce del nuovo GDPR

GDPR

Accountability

Il dato diventa un bene che va tutelato a sé, e **il titolare diventa il solo responsabile dei trattamenti** e deve dimostrare di di aver valutato i rischi connessi al trattamento dei dati e di aver adottato tutte le misure idonee a garantire la tutela del dato: tenendo conto degli strumenti tecnologici a disposizione del titolare, dei costi di attuazione e dei rischi, il titolare dovrà mettere in atto misure tecniche e organizzative adeguate a garantire la protezione dei dati (trattare solo i dati necessari alle proprie finalità e limitarne l'accesso alle sole persone che ne fanno uso per la propria attività all'interno dell'organizzazione).

Per dimostrare la conformità del trattamento il titolare deve adottare la **Privacy by default**, cioè un sistema di corretta organizzazione, documentazione e tracciabilità durante il trattamento dei dati (processi gestionali e policy interne, il registro dei trattamenti o l'adesione a codici di condotta o meccanismi di certificazione), e la **Privacy by design,** cioè l'uso di sistemi informatici con il quale vengano trattati dati personali che dev'essere progettato e realizzato in modo tale da garantire la tutela del dato stesso.

DATI

Dati personali

Qualunque informazione relativa ad una persona fisica identificata o identificabile, anche indirettamente, attraverso altre informazioni.

Dati sensibili

Dati personali idonei a rivelare l'origine razziale ed etnica, le convenzioni religiose e filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti e sindacati o ad associazioni e organizzazioni a carattere religioso, filosofico, politico, sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati giudiziari

Dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale.

Dati sanitari

Dati personali 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.

Dati biometrici

Dati personali che consentono o confermano l'identificazione della persona in maniera univoca.

Dati genetici

Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite che forniscono informazioni univoche sulla fisiologia o lo stato di salute di detta persona fisica

SOGGETTI

Titolare

Persona, fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità e modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza

Responsabile

Persona, fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo, preposti dal Titolare al trattamento

Incaricato

Persona fisica autorizzata a compiere operazioni di Trattamento sulla base delle istruzioni ricevute dal Titolare e/o dal Responsabile

Interessato

Persona fisica titolare dei dati

ALTRE DEFINIZIONI

Trattamento

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di Dati personali, anche se non registrati in una banca dati

Gli adempimenti necessario e/o opportuni per gli esercenti la professione di ostetrica

Predisposizione informativa e raccolta del consenso

Nomina del *Data Protection Officer*

Conservazione dati

Tenuta del registro trattamenti

Organizzazione Studio e nomina responsabili esterni

Art. 6 GDPR

- Un trattamento di Dati Personali è lecito se e nella misura in cui è permesso ai sensi del GDPR. Se il Titolare del Trattamento non agisce in virtù di una base giuridica legittima prevista dal GDPR e non sussistono esenzioni, il trattamento è illecito e si rischia di incorrere in sanzioni.
- ***Attenzione***: il Titolare, indipendentemente dalla propria natura giuridica e dal settore in cui opera, è sempre tenuto a trattare i Dati in modo lecito. Il GDPR obbliga i Titolari ad esporre nell'informativa privacy le ragioni che giustificano il trattamento e gli scopi del Trattamento.

La liceità del trattamento

Le condizioni di legittimità indicate dal GDPR sono 4:

- Il **consenso** e cioè la volontà libera, specifica e informata manifestata dall'Interessato affinché i suoi Dati personali siano fatti oggetto di Trattamento.
- L'esecuzione di un contratto.
- L'adempimento di un obbligo legale.
- L'esecuzione di un compito di interesse pubblico.
- Il perseguimento di un interesse legittimo (questa condizione non si applica alla PA nell'adempimento e svolgimento delle sue funzioni).

Il trattamento di Dati Sensibili presuppone **sempre** il consenso dell'interessato.

L’informativa

Documento contenete le informazioni che il Titolare deve fornire all’Interessato per chiarire se quest’ultimo è obbligato o meno a rilasciare i dati personali, le conseguenze di un eventuale rifiuto al rilascio dei dati personali, quali sono le finalità e le modalità del trattamento, i soggetti che entrano in contatto con i suoi dati personali, come circolano i dati personali e in che modo esercitare i diritti riconosciuti dal GDPR

Il contenuto dell'informativa

- identità e dati di contatto del Titolare;
- I dati di contatto del DPO;
- Finalità e base giuridica del trattamento;
- Destinatari e categorie di destinatari dei dati trattati;
- Il periodo di conservazione dei dati;
- I diritti dell'interessato.

Il consenso

- Il consenso deve essere **specifico**, cioè intellegibile. A fronte di una chiara indicazione della Finalità e delle conseguenze del Trattamento, il Consenso viene rilasciato con riferimento a detto Trattamento specifico.
- Il consenso deve essere **informato**: l'Interessato deve ricevere tutte le informazioni necessarie per capire in cosa consiste il Trattamento e per quali finalità è effettuato.
- Non si ritiene validamente ottenuto il Consenso se l'Interessato non ha scelto in modo **libero** e **genuino** di prestarlo o se non ha la **possibilità di rifiutarsi** al Trattamento dei Suoi Dati o se **non può revocarlo quando vuole** senza subire alcun danno.

Manifestazione e raccolta del Consenso

- Il GDPR chiarisce che il Consenso è il risultato di un **comportamento attivo** o di una **dichiarazione positiva** dell'Interessato.
- E' riconosciuta la validità di un diffuso numero di metodi per raccogliere il consenso dell'Interessato.
- E' invece **esclusa** l'ipotesi del **silenzio – assenzo**, delle **caselle pre-selezionate su internet** e **l'inattività** come forme lecite di raccolta del consenso.

Manifestazione e raccolta del Consenso

Consigli Pratici

- I titolari devono assicurarsi che gli Interessati siano debitamente informati, prima di rilasciare il Consenso, su che cosa consiste il Trattamento;
- I Titolari del Trattamento sono tenuti ad adottare meccanismo di raccolta del Consenso che siano ben parametrati sulla natura del consenso richiesto,
- Non possono essere previsti meccanismi di silenzio-assenso, acquiescenza passiva o box preselezionati sui siti internet del Titolare.
- I Titolari sono obbligati a prevedere meccanismi che assicurino agli interessati la revoca immediata del Consenso

Manifestazione e raccolta del Consenso

Consigli Pratici

- Il consenso della persona al trattamento dei dati sanitari deve essere pertanto raccolto all'inizio del rapporto assistenziale e vale, per le stesse finalità per le quali è stato autorizzato, a tempo indeterminato. Questo significa che se l'ostetrica intende utilizzare i dati della paziente per finalità diverse e ulteriori rispetto a quelle originarie deve integrare l'informativa e acquisire un ulteriore consenso specifico.

Attenzione

- Il consenso al **trattamento dei dati** non implica e non presuppone il **consenso all'atto medico**.

SOGGETTI

Data Protection Officer (DPO)

Ha compiti specifici:

- Informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento
- Predisporre relazioni periodiche per il management
- Sorvegliare l'osservanza del Regolamento e di tutte le altre disposizioni anche nazionali in materia di protezione dei dati
- Vigilare che il Titolare ed il Responsabile conferiscano nomine a soggetti adeguati
- Verificare l'adozione di policy adeguate
- Sensibilizzare e formare il personale che partecipa ai trattamenti e alle attività di controllo
- Assistere il Titolare nello svolgimento della valutazione di impatto
- Predisporre e mantenere aggiornato il registro dei trattamenti
- Cooperare con l'Autorità di controllo

SOGGETTI

Data Protection Officer (DPO)

E' obbligatoria solo in alcuni casi:

- Se il titolare è un soggetto pubblico;
- Se l'attività principale del Titolare consiste in trattamenti che, per loro natura, ambito di applicazione o finalità comportano il monitoraggio regolare e sistematico degli interessati "su larga scala",
- se l'attività principale del Titolare consiste in trattamenti regolari e sistematici di dati particolari o giudiziari.

La nomina del DPO

E' obbligatoria solo in alcuni casi:

- Se il titolare è un soggetto pubblico;
- Se l'attività principale del Titolare consiste in trattamenti che, per loro natura, ambito di applicazione o finalità comportano il monitoraggio regolare e sistematico degli interessati "su larga scala",
- se l'attività principale del Titolare consiste in trattamenti regolari e sistematici di dati particolari o giudiziari.

Il *Considerando 91* prevede che studi medici, odontoiatrici e professionali con un solo titolare del trattamento dei dati personali dei pazienti **non sono obbligati a nominare il DPO**.

La nomina del DPO (*segue*)

Secondo il Garante per la Privacy "*nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), può risultare comunque fortemente raccomandato, ancorché non obbligatorio, procedere alla designazione di un RPD. In ogni caso, qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i RPD designati in via obbligatoria*".

La nomina del DPO è però suggerita dal Garante a ogni medico convenzionato con il SSN.

Il registro dei trattamenti

Il registro dei trattamenti contiene tutte le seguenti informazioni:

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, compresi i destinatari di paesi terzi od organizzazioni internazionali;

Il registro dei trattamenti (segue)

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;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Il registro dei trattamenti (segue)

Per ciò che concerne il trattamento dei dati sanitari, tutte le strutture sanitarie in qualitò di titolari del trattamento dati nonché tutte /e imprese che rivestono il ruolo di Responsabili de/ trattamento dati in quanto trattano dati particolari per conto di strutture sanitarie, dovranno dotarsi obbligatoriamente di un registro dei trattamenti.

Sono da ritenersi esclusi da tale elenco gli studi sanitari professionali che non trattano dati particolari per conto di strutture sanitarie.

Consigli pratici

Si consiglia, anche solo a titolo precauzionale, di creare e gestire tali registri.

L’organizzazione dello studio

- adottare soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno di strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;
- far rispettare appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere.
- adottare soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
- utilizzare tutte le possibili cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;

L’organizzazione dello studio

- assicurare il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;
- utilizzare i più opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;
- g) mettere in atto procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;
- i) sottoporre agli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

L’organizzazione dello studio

- assicurare il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;
- utilizzare i più opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;
- g) mettere in atto procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;
- i) sottoporre agli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

Misure di sicurezza informatica

- I software utilizzati devono essere sempre aggiornati.
- I Sistemi Informatici (ivi inclusi tutti i computer, altri dispositivi e i server) devono essere protetti da adeguati anti-virus di ultima generazione (quali, ad esempio, anti-virus "comportamentali"), firewall e software di sicurezza. Gli anti-virus, firewall e software di sicurezza dovranno essere mantenuti aggiornati all'ultimo aggiornamento di tali software disponibile;
- I supporti esterni impiegati dagli Utilizzatori per trasferire file devono essere sottoposti a scansione anti-virus prima che un file possa esservi memorizzato. La scansione anti-virus dovrà essere effettuata automaticamente alla connessione o all'inserimento del supporto nel dispositivo

Misure di sicurezza informatica

- Qualsiasi file inviato a terzi tramite e-mail, su supporto fisico o con altri mezzi (ad esempio, FTP o cloud condiviso) deve essere sottoposto a scansione anti-virus prima di essere inviato o nel corso del processo di invio, a seconda dei casi;
- i Sistemi Informatici devono essere collocati in locali che possano essere chiusi in modo sicuro quando non utilizzati;
- I Sistemi Informatici non destinati al normale uso da parte degli Utilizzatori (inclusi, ma non limitati a, server, apparecchiature di rete e infrastruttura di rete) devono essere collocati, ove possibile, in stanze protette e climatizzate e/o in armadi chiusi a chiave. A tali locali possono accedere soltanto i soggetti appositamente autorizzati.

Misure di sicurezza informatica

- Sui Sistemi Informatici devono essere implementate le misure di segregazione (quali, ad esempio, la segregazione delle aree all'interno del *server* e delle reti) e di limitazione di accesso;
- devono essere definiti profili di abilitazione e identificazione basati su credenziali e password di protezione che consentano agli Utilizzatori di accedere ai Sistemi Informatici nei limiti di quanto loro necessario allo svolgimento delle relative mansioni lavorative, ovvero dei compiti e dei servizi di cui sono stati incaricati.

Misure di sicurezza informatica

- Le password utilizzate sui Sistemi Informatici e nei profili di abilitazione e identificazione devono, laddove il software, il computer o il dispositivo lo consentano:
  - essere almeno sette caratteri;
  - contenere una combinazione di almeno tre dei seguenti caratteri: lettere maiuscole, lettere minuscole, numeri e altri caratteri non alfanumerici;
  - essere modificate almeno ogni mese;
  - qualora modificate, essere diverse dalle password usate in precedenza;
  - non essere ovvie o facilmente intuibili o identificabili (ad esempio, compleanni o altre date significative, nomi, eventi o luoghi, ecc.);
  - essere create dai singoli Utilizzatori.
- I Sistemi Informatici con display o altri dispositivi esterni (ad esempio, mouse, tastiera, touchscreen ecc.) devono essere protetti, se possibile, mediante un sistema cdi blocco che si attivi automaticamente dopo 15 minuti di inattività.

La contitolarità

- Quando, con riferimento ad un singolo Trattamento, due o più entità decidono e determinano congiuntamente le Finalità e i mezzi del Trattamento, queste sono **contritolari** del Trattamento.
- In molte circostanze, un Trattamento viene ad articolarsi in una serie di operazioni e/o attività svolte ciascuna delle quali da due o più Titolari differenti, ma tra loro collegati.
- Il GDPR obbliga i contitolari a sottoscrivere un accordo interno con cui vengono ripartite le responsabilità e stabiliti i ruoli dei soggetti.
- Il contenuto dell'accordo deve essere sintetizzato e messo a disposizione degli Interessati.
- Il GDPR rende i contitolari pienamente responsabili nei confronti dell'Interessato.

Fine

Avv. Alessandro Mosti
Viale Cadorna, 50
0583.955903
392.9281205
alessandro.mosti@gmail.com