GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

L'adeguamento a GDPR e decreto 101/2018 comporta una serie di obblighi per gli studi medici e odontoiatrici. Una guida per i professionisti sanitari verso l'adempimento degli obblighi che la normativa impone o, in alcuni casi, consiglia loro

Con il Regolamento Europeo 2016/679 (GDPR) e con l'entrata in vigore del D. Lgs. 101/2018, gli studi medici e odontoiatrici si trovano a dover adempiere ad una serie di obblighi che, a vario titolo, provocano diversi mutamenti organizzativi ed economici al loro interno. Vediamoli nel dettaglio.

La responsabilizzazione dello studio

Per comprendere il reale impatto degli obblighi che gravano sullo Studio medico e odontoiatrico è fondamentale partire da un concetto cardine del GDPR: il principio di responsabilizzazione (o di "accountability"[1]). Fondamentale perché lo studio è pienamente responsabile delle scelte e delle azioni messe in campo (art. 5.2 GDPR), e deve "darne conto" ai pazienti interessati al trattamento, al Garante Privacy[2] e all'autorità giudiziaria. Sono concetti che vanno al di là di semplici costrutti giuridici, anzi. Col "nuovo corso" europeo non c'è nulla di più serio della nozione di "responsabilizzazione", poiché lo Studio diventa, nella maggior parte dei casi, unico centro di imputazione per qualsiasi trattamento non a norma di legge.

Lo studio titolare del trattamento

Lo Studio medico e odontoiatrico è Titolare del trattamento dei dati ossia, la persona (fisica o) giuridica che determina le finalità e le modalità del trattamento dei dati. È, quindi, Titolare del trattamento lo Studio medico e odontoiatrico che tratta i dati dei pazienti per finalità di anamnesi, diagnosi, terapia sanitaria, prevenzione e riabilitazione con strumenti informatici (ad es. PC) e/o cartacei (ad es. Modulistica).
In alcuni casi è possibile che il singolo medico o il singolo odontoiatra siano essi stessi Titolari del trattamento dei dati; questo può accadere quando, generalmente, lo Studio è composto dal singolo medico o dal singolo odontoiatra. Casi, ovviamente, più rari in quanto nella generalità delle situazioni la composizione dello Studio è più ampia.
Diffusa è la figura del Contitolare del trattamento dei dati. Ai sensi dell'art. 26 GDPR quando due o più titolari determinano congiuntamente le finalità e le modalità del trattamento, essi sono Contitolari del trattamento. La contitolarità viene sancita da un accordo interno che delinea le rispettive responsabilità in merito all'ottemperanza al GDPR. Un esempio classico di contitolarità è lo Studio Medico Associato (due o più medici/odontoiatri che trattano dati autonomamente, pur determinando e condividendo le medesime finalità e modalità del trattamento).
In ogni caso è fondamentale tenere presente il binomio finalità-modalità del trattamento in rapporto con il concetto di "responsabilizzazione". Un rapporto che non deve mai sfuggire al professionista sanitario.

Le informazioni e i diritti del paziente

Se il binomio Responsabilizzazione-Titolare del trattamento rappresenta il basamento del GDPR, una delle colonne portanti del medesimo è la coppia Informazioni-Diritti.
Il GDPR su questo punto non transige: il paziente va informato e i suoi diritti vanno agevolati nella maniera più efficace possibile. Ma come va informato il paziente in merito ai suoi diritti?

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

Innanzitutto vanno eliminate tutte quelle informative[3] privacy che fanno parte del "vecchio corso"; quindi via il copia-incolla del testo di legge, via i caratteri illeggibili, via il linguaggio "da avvocato" e lo stile "grigio". L'art. 12 GDPR su questo è cristallino, per cui è necessario:

- Utilizzare un linguaggio semplice e chiaro con una forma intellegibile, ossia comprensibile "dall'uomo medio" e, quindi, dalla maggior parte dei pazienti dello Studio. Raccomandazione: si faccia riferimento all'età media e al livello di istruzione.
- Utilizzare una forma concisa. Le informative privacy "chilometriche" e vuote di significato altro non fanno che scoraggiare il paziente alla lettura, e questo è un problema risaputo.
- Utilizzare una forma trasparente. Bisogna fare in modo che ciò che si scrive nell'informativa privacy risponda a realtà: meglio scrivere qualcosa di essenziale ma veritiero, che qualcosa di bello e pomposo ma non rispondente alla realtà.
- Utilizzare una forma facilmente accessibile. Raccomandazione: non inserire l'informativa privacy solo ed unicamente nella modulistica di Studio, poiché molto raramente un paziente legge l'informativa in prossimità della compilazione e firma di un modulo. Molto più efficace è affiggere l'informativa in sala d'attesa, o fornirla sotto forma di dépliant. La sua presenza sul sito web dello Studio, o sui social dello stesso sarebbe poi, indubbiamente, un must (si veda il punto 10).
- Ulteriore raccomandazione: non sottovalutare l'uso del colore e di determinati caratteri nella redazione di informative privacy. Più si cattura la curiosità del paziente, più l'efficacia dell'informativa raggiunge il suo scopo.

Ma cosa deve contenere un'informativa ex art. 13 GDPR? [4] Oltre al linguaggio e alla forma, anche alcuni elementi:

- L'identità e i dati di contatto del Titolare del trattamento. Nulla di più semplice: inserire la ragione sociale e i dati di contatto dello Studio. Nel caso di Titolare del trattamento persona fisica inserire i propri dati anagrafici in luogo della ragione sociale. Raccomandazione: i dati di contatto devono corrispondere al vero e devono essere sempre aggiornati.
- I dati di contatto del DPO (si veda il punto 9). Inserirli solo se richiesto dalla norma ovvero inserirli nel caso in cui lo Studio avesse deciso di nominarne uno facoltativamente.
- Le finalità del trattamento. La domanda alla quale rispondere è: a cosa mi serve trattare questi dati personali? Nel caso dello Studio medico e odontoiatrico la risposta è pressappoco questa: "per finalità di anamnesi, diagnosi, terapia sanitaria, prevenzione e riabilitazione", ossia per tutti i casi in cui è necessario il (e non si può prescindere dal) trattamento dei dati personali del paziente. Raccomandazione: inserire le finalità che effettivamente si perseguono, che possono essere anche diverse da quelle precedentemente elencate.
- La base giuridica del trattamento. Si veda il punto 4.
- I destinatari del trattamento. La domanda alla quale rispondere è: quale persona fisica, giuridica, autorità pubblica o organismo riceve comunicazione dei dati personali? Si può far riferimento a soggetti interni allo Studio (es. collaboratori), o soggetti esterni che effettuano trattamenti per conto dello Studio (es. commercialista) ovvero Enti pubblici (es. Regione). In ogni caso è necessario specificare nell'informativa privacy almeno la categoria di riferimento dei destinatari.

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

- Il trasferimento all'estero di dati verso paesi terzi o organizzazioni internazionali. Caso non comune tra la maggior parte degli Studi medici e odontoiatrici, ma non impossibile. In questo caso se vi fosse necessità (ed intenzione) di trasferire alcuni dati verso paesi terzi (ad es. extra UE) o organizzazioni internazionali bisogna inserirlo nell'informativa privacy. È, inoltre, necessario inserire la presenza o l'assenza di decisioni di adeguatezza della Commissione Europea. [5]
- Il periodo di conservazione dei dati o i criteri utilizzati per determinarne il periodo. Lo Studio medico e odontoiatrico deve inserire nell'informativa privacy la tempistica di conservazione delle diverse categorie di dati personali trattati. È del tutto chiaro che un dato di contatto (es. numero di cellulare) non può essere conservato per un periodo pari a quello di un referto o di una cartella clinica. È fondamentale quanto meno stimare diversi periodi di conservazione per le diverse tipologie di dati trattati (anagrafici, salute, genetici ecc.).
- I diritti del paziente sui suoi dati personali. Questa è la parte più importante dell'informativa privacy, quindi lo Studio deve dedicarvi la massima attenzione. Importante: sono diritti esercitati dal paziente senza alcuna formalità e gratuitamente (salvo richieste reiterate, eccessive o infondate); lo Studio deve ottemperare alle richieste senza ingiustificato ritardo, al massimo entro un mese dal ricevimento delle stesse (prorogato di due mesi in caso di richieste numerose o complesse). Infine si risponde, ove possibile, alle richieste del paziente nella stessa loro forma: a richieste cartacee si risponde in maniera cartacea, a richieste elettroniche si risponde in maniera elettronica.

I diritti del paziente sui suoi dati personali

- Ai sensi dell'art. 15 GDPR il paziente interessato ha il diritto di ottenere (gratuitamente) dallo Studio la conferma che è in atto – o meno – un trattamento di dati personali che lo riguarda, di ottenere l'accesso a questi dati ed alcune informazioni già previste (e garantite) nell'informativa[6].
- Ai sensi dell'art. 16 GDPR il paziente interessato ha il diritto di ottenere la rettifica di dati personali inesatti ovvero l'integrazione di dati personali incompleti.
- Ai sensi dell'art. 17 GDPR il paziente interessato ha il diritto alla cancellazione dei suoi dati nel caso che (a suo avviso) non siano più necessari rispetto alle finalità di raccolta;
- nel caso revochi il suo consenso e manchino altre basi giuridiche (si veda il punto 4); nel caso il paziente si opponga al trattamento e non vi siano altri motivi legittimi per procedere con lo stesso;
- nel caso i dati siano trattati illecitamente da parte dello Studio;
- nel caso i dati debbano essere cancellati per adempiere ad un obbligo di legge cui è soggetto lo Studio.

In tutti questi casi lo Studio dovrà procedere alla cancellazione di tali dati (a prescindere se su supporto elettronico o cartaceo) senza ingiustificato ritardo.

Non si applica il diritto alla cancellazione nell'ambito dello Studio medico e odontoiatrico quando:

- vi è un obbligo di legge da rispettare, un compito da svolgere nel pubblico interesse ovvero l'esercizio di pubblici poteri cui può essere investito lo Studio;

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

- non si applica quando vi sono motivi di interesse pubblico nel settore della sanità pubblica (es. trattamento necessario per finalità di medicina preventiva, medicina del lavoro, diagnosi, assistenza, terapia sanitaria ecc.);
- non si applica per fini di archiviazione nel pubblico interesse e ricerca scientifica nella misura in cui il diritto alla cancellazione non pregiudichi tali obiettivi;
- ed infine non si applica per l'accertamento, l'esercizio o la difesa di un suo diritto in sede giudiziaria (art. 24 Cost.). [7]

Limitazione del trattamento dei dati personali

Ai sensi dell'art. 18 GDPR il paziente interessato ha il diritto di ottenere la limitazione del trattamento dei dati personali che lo riguardano quando:

- contesta l'esattezza dei dati personali;
- il trattamento è illecito;
- il paziente ha necessità di utilizzare i suoi dati per l'accertamento, l'esercizio o la difesa di un suo diritto in sede giudiziaria benché lo Studio non abbia più bisogno di questi dati;
- infine, quando il paziente si oppone al trattamento dei suoi dati.

Portabilità dei dati

Ai sensi dell'art. 20 GDPR[8] il paziente interessato ha il diritto alla portabilità dei suoi dati, ossia di ricevere dallo Studio i dati personali che lo riguardano, e ha il diritto di chiedere allo Studio di trasmetterli ad altro titolare del trattamento (es. altro Studio medico). Lo Studio deve consegnare i dati – o trasmetterli – in un formato strutturato, di uso comune e leggibile da dispositivo automatico.

Il paziente può esercitare il diritto alla portabilità dei suoi dati a due condizioni:

- che vi sia la presenza di una base giuridica in alternativa tra consenso e contratto;
- che il trattamento sia effettuato con mezzi automatizzati (non è possibile la portabilità di dati contenuti in modulistica cartacea). Chiaramente l'esercizio del diritto alla portabilità non pregiudica altri diritti (ad esempio, non pregiudica il diritto alla cancellazione ex art. 17 GDPR).
- Infine, ai sensi dell'art. 21 GDPR il paziente interessato ha il diritto di opporsi in qualsiasi momento al trattamento avente come basi giuridiche l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ovvero il legittimo interesse dello Studio medico e odontoiatrico.

Cosa deve includere l'informativa privacy

- L'informativa privacy deve inoltre contenere la possibilità che il paziente revochi il suo consenso – se tra le basi giuridiche che lo Studio utilizza vi è questa – in qualunque momento (e senza motivazioni). In questo caso è lecito il trattamento effettuato prima della revoca del consenso. Raccomandazione: siccome il consenso deve poter essere revocato con la stessa facilità con la quale è prestato, sarebbe utile che lo Studio adottasse una modulistica ad hoc per facilitare la revoca del consenso.

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

- L'informativa privacy deve contenere il diritto di proporre reclamo presso un'Autorità di Controllo. Raccomandazione: è consigliabile inserire nell'informativa direttamente il binomio Autorità di Controllo e Sito Web (ad esempio, Garante Privacy – https://www.garanteprivacy.it).
- L'informativa privacy deve specificare se la comunicazione di dati personali (ai destinatari) è un obbligo di legge o contrattuale, se il paziente ha l'obbligo di fornire tali dati e le possibili conseguenze nel caso in cui lo stesso non volesse procedere con la comunicazione.
- Infine, l'informativa privacy deve specificare se è in atto un processo decisionale automatizzato (art. 22 GDPR), con la logica utilizzata, l'importanza e le conseguenze di tale trattamento.

Importante: se lo Studio medico e odontoiatrico avesse necessità di trattare ulteriormente i dati personali dei suoi pazienti per un'altra finalità (es. passaggio da finalità di cura a finalità di ricerca), sarà necessario che lo Studio informi i suoi pazienti in merito a questo ulteriore trattamento.

La perdita di esclusività del consenso in ambito sanitario

Com'è noto, il vecchio Codice Privacy si fondava su una sorta di esclusività del consenso in ambito sanitario: era consuetudine infatti, che accanto al consenso al trattamento sanitario ci fosse il consenso al trattamento dei dati personali. Un binomio inossidabile. Con il GDPR non è più così. Il consenso di oggi sembra una sorta di primus inter pares, ossia una base giuridica che ha sì il suo indiscutibile peso, ma non ad un livello superiore ad altre.

Ma su quali basi giuridiche si fonda la liceità del trattamento dei dati nello Studio medico e odontoiatrico?

La base giuridica per eccellenza nel trattamento dei dati particolari[9] relativi alla salute è presente nell'Art. 9.2 h) GDPR. In tale articolo si dispone che: è lecito il trattamento dei dati particolari per finalità di medicina preventiva, 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 [...] ovvero conformemente al contratto con un professionista della sanità [...]. In pratica, non è più necessario il "consenso privacy" accanto al consenso al trattamento sanitario, in quanto è superfluo trovarsi davanti a due autorizzazioni per la medesima finalità di cura, diagnosi, assistenza sanitaria ecc. Il trattamento dei dati personali è strumentale al trattamento sanitario, quindi è lecito "di per sé". A garanzia di quanto affermato vi è l'art. 9.3 GDPR, il quale dispone che è possibile utilizzare la base giuridica di cui all'Art. 9.2 h) solo se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale [...] o da altra persona anch'essa soggetta all'obbligo di segretezza [...].

Raccomandazioni: nell'informativa privacy dello Studio (punto 3) si faccia riferimento a quanto qui esposto, inserendo chiaramente tale base giuridica.

Al secondo gradino del podio è inevitabile inserirvi il consenso (art. 6.1 a, art. 9.1 a GDPR) che, come anticipato, riveste sempre un suo peso. Nello Studio è possibile utilizzare il consenso per altri trattamenti ed altre finalità. Ad esempio, per comunicare con il paziente interessato tramite telefono, sms, ma anche messaggistica

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

istantanea o per mail è necessario un autonomo consenso, poiché sono ultronei rispetto alla fattispecie di cui all'Art. 9.2 h). Quindi nell'informativa privacy bisognerà aggiungere quest'altra base giuridica per queste diverse finalità.

Tuttavia, è bene sottolineare che il consenso è disciplinato rigidamente nel GDPR, che gli dedica l'intero art. 7. Tra le disposizioni:

- Lo Studio deve dimostrare che il paziente interessato ha prestato il proprio consenso;
- Ad ogni finalità del trattamento deve esserci un autonomo consenso;
- Il consenso deve essere comprensibile, facilmente accessibile, con linguaggio semplice e chiaro e chiaramente distinguibile da altre materie (e finalità);
- Il consenso è revocabile con la stessa facilità con la quale è prestato, in qualsiasi momento;
- La revoca del consenso non pregiudica il trattamento posto in essere sino ad allora;
- Il consenso è sempre informato (ecco perché l'informativa privacy deve essere assolutamente cristallina);
- Infine, nel caso dello Studio medico e odontoiatrico, il consenso deve essere esplicito (art. 9.2 a – ad esempio con dichiarazione scritta o elettronica).

Infine è possibile che lo Studio tratti più o meno occasionalmente dati personali mediante altre basi giuridiche:

- Art. 9.2 c) quando il trattamento dei dati è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica (anche 6.1 d) qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso (classico esempio, il paziente in codice rosso in Pronto Soccorso);
- Art. 6.1 b) quando il trattamento è necessario all'esecuzione di un contratto in cui l'interessato è parte (il rapporto tra medico e paziente può essere disciplinato da un contratto);
- Art. 6.1 c) quando il trattamento è necessario per adempiere ad un obbligo legale cui è soggetto lo Studio (ad esempio, invio di alcuni dati al SSR);
- Art. 6.1 e) quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- Ed infine, Art. 6.1 f) quando il trattamento è necessario per il perseguimento del legittimo interesse[10] del titolare del trattamento o di terzi.[11]

È il caso di ribadire che lo Studio Titolare del trattamento valuta autonomamente le basi giuridiche che vuole utilizzare: per il principio di responsabilizzazione è possibile utilizzare altre basi giuridiche, l'importante è saper giustificare le scelte.

La sicurezza dei dati personali

Ed eccoci al punctum dolens di ogni Studio medico e odontoiatrico dall'alba dei tempi (privacy) sino ad oggi: come garantire la sicurezza dei dati personali dei pazienti? Il GDPR su questo non fa sconti. Innanzitutto, bisogna dimenticare la coppia misure minime / misure idonee di cui al vecchio Codice. Con il GPDR le uniche misure di sicurezza ammesse sono quelle "adeguate".

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

L'art. 32 GDPR dispone che per approntare delle adeguate misure di sicurezza bisogna tener conto dello stato dell'arte (avanzamento tecnologico), dei costi di attuazione (delle misure di sicurezza), della natura, dell'oggetto, del contesto e delle finalità del trattamento dei dati, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (porre in essere, quindi, un'analisi del rischio sui dati personali trattati). Il tutto per garantire un livello di sicurezza adeguato al rischio. Tra le "soluzioni" che l'art. 32 elenca – in maniera non esaustiva – vi sono:

- la pseudonimizzazione[12] e la cifratura[13] dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (ovvero, anche la capacità del sistema di resistere e reagire);
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (es. backup / disaster recovery[14]);
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Inoltre nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento 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. Inoltre, punto importante, lo Studio Titolare del trattamento fa sì che chiunque agisca sotto la Sua autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso (si veda il punto 6).

È sempre utile rammentare quelle che sono le misure imprescindibili per uno Studio medico e odontoiatrico che, in un certo senso, precedono quanto previsto dall'art. 32 GDPR:

- Controllo degli accessi alle postazioni PC, nonché ad altri terminali, mediante username e password per ogni singolo operatore;
- Username e password devono essere perfettamente memorizzati, non vanno scritti su carta e collocati a vista presso la postazione PC, sono personali e non cedibili a nessuno;
- Ogni volta che si abbandona la postazione PC, anche per pochi secondi, va effettuata la disconnessione dal terminale (ad esempio, Logo Windows + L);
- La password va cambiata periodicamente e non oltre 90 giorni;
- Su ogni PC e terminale vanno installati Antivirus e Firewall con licenze d'uso originali (preferibilmente, non affidarsi a software gratuiti);
- Antivirus e Firewall devono essere aggiornati quotidianamente;
- Dotarsi di soluzioni di crittografia / pseudonimizzazione per gli archivi elettronici;
- Porre in essere backup periodici.
- Replicare le stesse misure di sicurezza sui terminali mobili (smartphone, tablet ecc.).

Cosa succede in caso di data breach

Ma cosa succede se lo Studio subisce un Data Breach (Violazione di dati personali – Artt. 33 e 34 GDPR)?[15]

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

In caso di Data Breach, lo Studio medico e odontoiatrico deve, senza ingiustificato ritardo e non oltre 72 ore dal momento in cui ne è venuto a conoscenza, notificare la violazione al Garante Privacy, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche[16]. Oltre le 72 ore è necessario allegare alla notifica il motivo del ritardo.

Cosa contiene la notifica del Data Breach al Garante Privacy?

- Descrizione dettagliata del Data Breach;
- Categorie (pazienti e non pazienti) e numero approssimativo di interessati;
- Categorie e numero approssimativo di registrazioni dei dati personali;
- Dati di contatto dello Studio per tutte le informazioni richieste dal Garante Privacy;
- Descrizione delle probabili conseguenze del Data Breach;
- Descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio.

In ogni caso, a prescindere dalla necessità di notifica o meno di un Data Breach, lo Studio deve documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente al Garante Privacy di verificare il rispetto di quanto disposto dal GDPR.

Il personale dello studio e la sua formazione

Verità lapalissiana è che lo Studio medico e odontoiatrico è quasi sempre composto da altro personale, oltre al singolo medico e al singolo odontoiatra. Che si tratti della segretaria di studio medico, dell'assistente professionista sanitario o dell'assistente alla poltrona di studio odontoiatrico, la maggior parte delle figure professionali che compongono lo Studio tratta dati personali.

L'art. 32.4 GDPR impone che chiunque agisca sotto l'autorità del Titolare del trattamento, e abbia accesso ai dati personali, non tratti i dati se non è istruito in tal senso dal Titolare del trattamento. L'art. 2-quaterdecies del Codice Privacy[17] afferma che il Titolare del trattamento può prevedere, sotto la sua responsabilità e nell'ambito del suo assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità. Inoltre, il Titolare sceglie le modalità più opportune per autorizzare al trattamento tali persone fisiche.

Quindi, da un lato abbiamo il GDPR con il termine "istruito", dall'altro il Codice Privacy con i termini "attribuzione" e "autorizzare". Da un lato lo Studio può autorizzare come meglio crede (responsabilizzazione) il proprio personale al trattamento dei dati, mediante l'attribuzione di specifici compiti e funzioni; dall'altro tale personale deve essere istruito, ossia deve comprendere la reale portata dell'autorizzazione. In altre parole, il personale autorizzato deve essere formato.

Solitamente la formazione è l'ultima ruota del carro quando uno Studio medico e odontoiatrico provvede con l'adeguamento al GDPR. In realtà dovrebbe essere una priorità: avere degli operatori che comprendono l'importanza di trattare adeguatamente i dati personali espone a rischi privacy e di sicurezza nettamente minori, e questo è un indubbio vantaggio per lo Studio.

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

Raccomandazioni: finanziare un corso privacy – preferibilmente sanitario – al proprio personale è una scelta vincente per lo Studio. Inoltre, prendendo in prestito il "diktat" dell'art. 28.3 b) – si veda il punto 7) – si consiglia di fare in modo che gli operatori dello Studio si impegnino, con apposito atto firmato, alla riservatezza circa le informazioni apprese all'interno del luogo di lavoro (sia privacy, sia know-how aziendale).

Gli operatori esterni responsabili del trattamento

Ogni Studio medico e odontoiatrico ha a che fare con soggetti esterni che trattano dati personali per suo conto. Si prenda, ad esempio, il caso del commercialista che cura la gestione contabile, la ditta di pulizie che sanifica i locali, o la ditta farmaceutica che fornisce i suoi presidi. Un novero di diversi soggetti che possono, e in taluni casi devono, trattare dati personali.
In questo caso si parla di rapporto tra lo Studio Titolare del trattamento ed il terzo Responsabile del trattamento, il quale tratta i dati per conto del Titolare. Il loro rapporto è rigidamente disciplinato dagli artt. 28 e 29 GDPR.
Questo rapporto deve essere sancito da un contratto o da un altro atto giuridico che abbia la caratteristica di vincolare il Titolare al Responsabile. Raccomandazione: sarebbe meglio che al contratto di fornitura seguisse in parallelo un contratto/atto vincolante sul trattamento dei dati; se vi sono già contratti di fornitura in essere, stipulare immediatamente i rispettivi contratti/atti vincolanti sul trattamento dei dati.
L'art. 28 GDPR non fa sconti a nessuno: per "delegare" un trattamento il fornitore deve fornire delle "garanzie sufficienti" di compliance al GDPR (in primo luogo, misure adeguate e diritti dell'interessato). E la valutazione sul possesso di queste garanzie (come tutte le valutazioni in seno al GDPR e al principio di responsabilizzazione) la fa lo Studio, nel nostro caso. Raccomandazione: se possibile, scegliere il fornitore che si presenta già "GDPR compliant"; in alternativa, valutare attentamente il fornitore nel rapporto costi-benefici (in ambito privacy). Il che non è sempre facile.
Il fornitore dello Studio, che riveste la qualifica di Responsabile del trattamento, non può ricorrere ad un "subfornitore – subresponsabile del trattamento" senza la previa autorizzazione scritta dello Studio medico e odontoiatrico. Inoltre l'autorizzazione dello Studio può essere specifica o generale e, in quest'ultimo caso, il fornitore Responsabile del trattamento informa lo Studio Titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri subresponsabili, dando così allo Studio l'opportunità di opporsi a tali modifiche.

Ma quali sono i contenuti che deve possedere il contratto/atto vincolante con il Responsabile del trattamento?

- Il fornitore Responsabile tratta i dati personali soltanto su istruzione documentata dello Studio Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale. Raccomandazione: si metta nero su bianco il margine di manovra che lo Studio dà al fornitore (generale o specifico).
- Il fornitore Responsabile garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza (si prenda spunto dal punto 6).
- Il fornitore Responsabile deve adottare tutte le misure di sicurezza adeguate richieste ai sensi dell'articolo 32 GDPR (punto 5).
- Il fornitore Responsabile si impegna a rispettare quanto sopra disposto per i subresponsabili del trattamento.

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

- Il fornitore Responsabile deve assistere lo Studio Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dei pazienti interessati (si veda il punto 3).
- Il fornitore Responsabile assiste lo Studio Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 GPDR (Misure di Sicurezza, Data Breach e Valutazione di Impatto – per quest'ultima si veda punto 9).
- Il fornitore Responsabile – su scelta dello Studio Titolare – deve provvedere alla cancellazione o alla restituzione di tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento; il fornitore Responsabile deve, inoltre, cancellare le copie esistenti, salvo che la legge non preveda la conservazione dei dati.
- Il fornitore Responsabile deve mettere a disposizione dello Studio Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi e deve consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati direttamente dallo Studio o da un altro soggetto da questi incaricato. Tolta la parte relativa alla richiesta di informazioni, che è limpida, le attività di revisione ed ispezione presso il fornitore devono essere molto ponderate da parte dello Studio. Le domande potrebbero essere: è necessario effettuare attività di revisione e ispezione presso i miei fornitori? Lo devo fare il mio Studio o posso delegare una società terza in mio conto (un responsabile del trattamento che revisiona/ispeziona un altro responsabile del trattamento)? Su questo è consigliabile valutare caso per caso: per il principio di responsabilizzazione è necessario rendere conto di ogni singola scelta.
- Inoltre, il fornitore Responsabile del trattamento informa immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati. Una disposizione tutt'altro che agevole per alcuni fornitori con cui lo Studio può intrattenere rapporti.

L'art. 28 GDPR è un articolo molto importante poiché, in un certo senso, "diluisce" il principio di responsabilizzazione di cui all'Art. 5.2 GDPR. Ciò non significa che con un contratto/atto vincolante lo Studio possa "appaltare" – oltre al trattamento dei dati – anche tutte le responsabilità connesse; bensì, seguendo scrupolosamente quanto dettato dall'art. 28 GDPR, è possibile quantomeno cedere una parte di responsabilità al fornitore, cosicché sarà lui a risponderne in determinate situazioni.[18]

Il registro delle attività di trattamento

Ulteriore novità del GDPR è il Registro delle Attività di Trattamento. Benché l'art. 30 GDPR parli di "Registri", in questo articolo si userà il singolare in rapporto alle necessità dello Studio medico e odontoiatrico.

Piccola nota: probabilmente alcuni medici e odontoiatri conosceranno la figura del DPS o Documento Programmatico sulla Sicurezza, che fino al 2012 era un rinomato sinonimo della frase "fare la privacy all'interno dell'azienda/ente". Tale documento, a revisione annuale, serviva a rendicontare quanto veniva fatto in azienda/ente in materia di protezione dei dati personali. Abrogato nel 2012, il DPS risorge come l'Araba Fenice

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

nel 2016 sotto la più potente forma di Registro, ai sensi del GDPR. E il Registro diventa un perno centrale del principio di responsabilizzazione.

Domanda: è un obbligo il Registro delle Attività di Trattamento per lo Studio medico e odontoiatrico? La risposta è Sì, e dipende essenzialmente dalle categorie di dati trattate. Il trattamento su base permanente di dati particolari e, principalmente, di dati relativi la salute (o sanitari), costituisce un obbligo al quale lo Studio non può sottrarsi.

Il Registro è tenuto in forma scritta e sotto la responsabilità del Titolare del trattamento.

Come procedere? A parere di chi scrive un foglio in formato xls/xlsx (Es. MS Excel) può andare più che bene. Ovviamente si possono utilizzare anche dei software ad hoc: il fine giustifica i mezzi.

I contenuti del Registro del Titolare del trattamento

Quali sono i contenuti del Registro del Titolare del trattamento? I suoi sette contenuti sono ben descritti dall'art. 30.1 GDPR.

- Primo punto (o casella di Excel). Inserire il nome e i dati di contatto del Titolare del trattamento. Quindi: ragione sociale dello Studio – o nome del medico/odontoiatra, nel caso di Titolare del trattamento persona fisica (si veda punto 2) – e dati di contatto (via, civico, CAP, città, provincia, contatto telefonico e mail). Nel caso lo Studio sia Contitolare del trattamento, inserirvi anche nome/i e dati di contatto del/i contitolare/i (si veda il punto 2). Inoltre, nella lontana ipotesi lo Studio abbia un DPO (si veda il punto 9), inserirvi il suo nome e i suoi dati di contatto.
- Secondo punto. Delineare in maniera compiuta quali sono le finalità del trattamento dei dati poste in essere nello Studio. È fondamentale che alla modifica/integrazione delle finalità nel Registro segua la modifica/integrazione dell'informativa privacy (si veda il punto 3). Quindi nella nostra casella Excel potremmo inserire sotto finalità, ad esempio: "trattamento dati per finalità di anamnesi, diagnosi, terapia sanitaria, prevenzione e riabilitazione".
- Terzo punto. Descrivere le categorie di interessati e le categorie di dati personali. Creando due caselle, nella prima si inseriscono le categorie di interessati, che per uno Studio medico e odontoiatrico sono solitamente i pazienti; nella seconda casella si inseriscono le categorie di dati personali trattati, che sono solitamente dati personali non particolari (es. anagrafici) e dati particolari (es. dati relativi la salute). L'uso dell'avverbio "solitamente" lascia volontariamente aperta la porta ad altre possibili categorie di interessati e di dati trattati, poiché è possibile che alcuni Studi trattino anche dati diversi per diverse categorie di interessati.
- Quarto punto. Descrivere le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi (se del caso) i destinatari di paesi terzi od organizzazioni internazionali. Anche qui è fondamentale che alla modifica/integrazione delle finalità nel Registro segua la modifica/integrazione dell'informativa privacy. Ad esempio, tra i destinatari figurerà il commercialista.
- Quinto punto. Ove applicabile, inserire i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate. Anche qui omogeneità con l'informativa privacy.

- Sesto punto. Inserire (ove possibile) i termini ultimi previsti per la cancellazione delle diverse categorie di dati, che non devono discostarsi da quanto previsto nell'informativa privacy. Ad esempio una cartella clinica ha una conservazione a tempo indeterminato, diversamente da un dato di contatto che può, ad esempio, essere conservato per 2 anni. Raccomandazione: valutare caso per caso la conservazione di ogni dato per ogni trattamento.
- Settimo punto. The best for last. Mettere in campo una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32.1 GDPR. Non è necessario mettere in campo una descrizione per ogni trattamento; una descrizione generale delle misure adeguate messe in campo va più che bene (si veda il punto 5).

Raccomandazione: tenere costantemente aggiornato il Registro delle Attività di Trattamento deve essere la priorità per lo Studio medico e odontoiatrico. Una revisione bimestrale o trimestrale è l'ideale

Valutazione d'impatto, dpo e trasferimento all'estero dei dati

Ad un esperto del settore inserire tre dei grandi pilastri del GDPR come la Valutazione d'Impatto, il DPO e il Trasferimento dati all'estero nello stesso paragrafo potrebbe far storcere il naso.
Scopo di questo punto però è di disciplinare le tre aree "facoltative e/o eventuali" che potrebbero (o meno) interessare lo Studio medico e odontoiatrico.

La Valutazione d'Impatto sulla Protezione dei Dati. Rubricata negli artt. 35-36 GDPR si configura come un'autonoma valutazione che il Titolare del trattamento pone in essere per analizzare la necessità, la proporzionalità e i rischi di un determinato trattamento dati per i diritti e le libertà delle persone fisiche. È richiesta in particolar modo in tre casi:

1. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
2. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
3. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (es. Videosorveglianza su larga scala).

Ora, la parte che potrebbe interessare maggiormente uno Studio medico e odontoiatrico è il b). Entrando "a gamba tesa" con la parte finale del considerando 91 GDPR si può affermare che "Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati."
Ma volendo occuparci non del singolo medico ma di più medici (nel singolo studio o in studi associati), cosa significa trattamento su larga scala? Secondo le Linee Guida del già "Gruppo dei Garanti Privacy europei"

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

(WP29)[19],[20] per determinare se un trattamento è svolto su larga scala si deve far riferimento al numero degli interessati, al volume di dati e/o tipologie di dati, alla durata dell'attività di trattamento e all'ambito geografico dell'attività di trattamento. In parole povere, se lo Studio tratta dati particolari su larga scala, è tenuto a porre in essere una Valutazione d'Impatto.

Cosa deve contenere la Valutazione d'Impatto

Ora, ammesso che è difficile che la maggior parte degli Studi medici e odontoiatrici tratti dati particolari su larga scala (prerogativa di un ospedale, ad esempio), vediamo cosa deve essere presente in una Valutazione d'Impatto a norma di legge. L'art. 35.7 dispone che la Valutazione d'Impatto deve contenere:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

In ogni caso è possibile avvalersi di un ottimo software messo a disposizione gratuitamente dal Garante francese CNIL e consigliato, nel suo utilizzo, dal Garante privacy italiano[21]. [22]

Il DPO

Destinatario della Sezione 4 (Artt. 37-38-39) GDPR, questa figura è stata introdotta come "supervisore" in materia di protezione dei dati personali all'interno delle aziende[23]. Anche qui, come per la Valutazione di Impatto, per la maggior parte degli Studi medici e odontoiatrici la presenza del DPO non è obbligatoria. Infatti l'obbligo scatta, ai sensi dell'art. 37 GDPR, solo nei seguenti casi:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Anche qui, quindi, con il termine larga scala si relega l'obbligatorietà della nomina del DPO ad una fetta marginale di Titolari del trattamento.
Tuttavia, se si volesse ugualmente procedere alla nomina di un DPO per il proprio Studio medico e odontoiatrico, sarà fondamentale affidarsi ad un soggetto che abbia una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati[24], e della capacità di assolvere i compiti di cui all'articolo 39 (informare, fornire consulenza, sorvegliare l'osservanza del GDPR, sensibilizzare e formare il personale, fornire un parere

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

sulla Valutazione d'Impatto, cooperare e fungere da punto di contatto con il Garante Privacy). Inoltre, il DPO può essere un dipendente dello Studio ovvero assolvere i suoi compiti in base a un contratto di servizi (ad esempio, con una società di consulenza che offre servizi DPO).

Il trasferimento all'estero dei dati

Altra eventualità (o residuale possibilità di concretizzazione per la maggior parte degli Studi) è il trasferimento all'estero dei dati. Come accennato in precedenza, per "estero" si intendono i paesi extra UE ed extra SEE.
Nel caso uno Studio abbia necessità di trasferire fuori dall'Unione Europea o fuori dallo Spazio Economico Europeo alcuni dati personali deve guardare a tre condizioni alternative.

- Presenza di una "decisione di adeguatezza". Se il paese verso cui lo Studio vuole trasferire i dati – allo stato attuale: Andorra, Argentina, Canada, Isole Faer Oer, Guernsey, Israele, Isola di Man, Jersey, Nuova Zelanda, Svizzera, Uruguay e USA[25] (e a breve Giappone[26]).
- In assenza di una "decisione di adeguatezza": il trasferimento dei dati personali deve essere effettuato sulla base di accordi contrattuali, stipulati tra il Titolare stabilito in Unione Europea e i soggetti destinatari dei dati stabiliti fuori dall'Unione Europea (quali ad esempio responsabili esterni o contitolari del trattamento), che forniscano garanzie adeguate agli utenti (esempio l'esercizio da parte di questi dei diritti a loro accordati dal GDPR). Per la conclusione di tali accordi contrattuali, la Commissione Europea ha emanato dei modelli standard;
- In assenza delle precedenti condizioni, l'articolo 49 GDPR, prevede alcune eccezioni – da utilizzare in limitate ipotesi e non per trattamenti continuativi – che giustificano comunque il trasferimento. Il trasferimento, può avvenire, alternativamente, soltanto se si verificano le seguenti condizioni:
- l'utente ha espresso esplicitamente il proprio consenso al trasferimento, una volta informato dal Titolare dell'assenza delle condizioni precedenti e degli eventuali rischi;
- il trasferimento è necessario per l'esecuzione di un contratto concluso tra l'utente e il Titolare stabilito in Unione Europea, ovvero nell'esecuzione di misure precontrattuali su istanza dell'utente.[27

Il rapporto dello studio con web e social media

È innegabile che, al giorno d'oggi, una parte dei trattamenti dei dati dello Studio medico e odontoiatrico si svolgano sul Web. Siti internet, Social Media e messaggistica istantanea sono utilizzati massivamente da molti professionisti sanitari. Ma come gestirli alla luce della normativa privacy?

Il sito web

Diversi Studi medici e odontoiatrici dispongono di un sito web, per diverse finalità. Che si tratti di pubblicizzare la propria attività, dare consigli su prevenzione, alimentazione o prenotazioni di prestazioni mediche, la normativa privacy è presente ovunque. Se il sito web è lo specchio dello Studio, bisogna fare in modo che segua un parallelo adeguamento al GDPR.

Alcune raccomandazioni:
Aggiornare la privacy policy del sito web e aggiornarla periodicamente. La privacy policy è l'informativa privacy del sito, quindi è fondamentale che abbia le stesse caratteristiche di cui al punto 3.

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

- Disciplinare i cookie del sito e la policy che li riguarda (banner compreso).[28]
- Disciplinare le newsletter, le prenotazioni e i contatti.
- Disciplinare i collegamenti con società di pagamento digitale e social media / applicazioni.

I social media

Particolare attenzione all'utilizzo dei Social Media (es. Facebook, Instagram, Twitter ecc.). Lo Studio che amministra una pagina di Social Media è in alcuni casi (addirittura) contitolare del trattamento (art. 26 GDPR). Con una recente sentenza la Corte di Giustizia dell'Unione Europea ha riconosciuto una contitolarità del trattamento in capo all'amministratore di una pagina ed alla stessa Facebook, dal momento che quest'ultima determina in via principale le finalità e le modalità del trattamento dei dati sulla propria piattaforma, puntualizzando anche che in caso di contitolarità la responsabilità non è equamente suddivisa tra i contitolari in maniera automatica, ma va determinata caso per caso. Tutti i soggetti che amministrano una pagina Facebook o altri social media rientrano nel campo di applicazione del GDPR, quindi devono valutare se stiano effettuando un trattamento dei dati personali in contitolarità con il social network. Tuttavia, è difficile immaginare un'applicazione fedele della norma del GDPR sulla contitolarità, in quanto difficilmente un titolare del trattamento può stipulare un accordo ai sensi dell'art. 26 GDPR con Facebook[29]. In ogni caso la pagina Facebook (o di altro Social) deve essere disciplinata come il sito web, quindi fondamentali devono essere le informazioni sul trattamento dei dati personali fornite nell'apposita sezione (ove possibile).

La messaggistica istantanea

È ormai consolidato che gli strumenti di messaggistica istantanea non danno alcuna garanzia legale sull'identità del mittente, quindi è sempre un rischio utilizzarli in ambito sanitario. In altre parole: mentre al telefono si ha un minimo di possibilità di identificare colui che sta dall'altra parte, perché magari 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. Nel rapporto medico-paziente è diffuso lo scambio di dati particolari (sensibili), soprattutto tramite Whatsapp e Facebook Messenger. Tuttavia non è consigliabile affidarsi a tali strumenti, sia per problemi di sicurezza delle informazioni[30], sia per problemi di non aderenza al GDPR[31] e Deontologia medica[32].

La videosorveglianza

Pur essendo un argomento molto disciplinato in dottrina, in una trattazione pragmatica della protezione dei dati in ambito medico e odontoiatrico non si può prescindere dalla Videosorveglianza. Soprattutto ora che il GDPR è entrato a gamba tesa in uno scenario totalmente basato sul Codice Privacy.
Indubbiamente molti Studi medici e odontoiatrici possiedono dispositivi di videosorveglianza: dal videocitofono (equiparato ad una telecamera, in quanto è possibile visualizzare in tempo reale chiunque nel suo raggio d'azione) all'impianto di ultima generazione, è sempre più pressante il bisogno di sicurezza del professionista sanitario.

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

Ad oggi la materia è ancora "monopolizzata" dal Provvedimento Generale 8 Aprile 2010[33], non essendoci stati interventi ulteriori da parte del Garante Privacy negli ultimi tempi. In attesa, quindi, di un intervento dell'Autorità in materia, il Provvedimento deve necessariamente subire delle "cesellature" per adeguarlo al GDPR.
In primis, l'informativa. La materia della Videosorveglianza ha la caratteristica della "doppia informativa", ossia un'informativa minima (cartello "Area Videosorvegliata") ed un'informativa completa. Se il cartello probabilmente sopravviverà nel formato attuale (indicazione del Titolare e delle finalità di trattamento), l'informativa completa – che lo Studio dovrà esporre all'interno – dovrà avere le medesime caratteristiche dell'informativa privacy di cui al punto 3.
Per quanto attiene la conservazione dei filmati, attenersi a quanto previsto dal Provvedimento Generale: "La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell´attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l´esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana". Inserire il periodo di conservazione all'interno dell'informativa completa.
Le misure di sicurezza da adottare in materia di Videosorveglianza devono rispettare l'art. 32 GDPR (si veda il punto 5). Parafrasando il Provvedimento Generale, i dati raccolti mediante sistemi di videosorveglianza devono essere protetti con adeguate misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.
Il Provvedimento dispone che devono essere adottate specifiche misure tecniche ed organizzative che consentano allo Studio medico e odontoiatrico di verificare l'attività svolta da parte di chi accede alle immagini o controlla i sistemi di ripresa. È fatta salva la necessità di avere differenti livelli di visibilità e trattamento delle immagini (rilevazione, anche mediante videocitofono). Sia i soggetti che rilevano (visualizzano le immagini in tempo reale), sia i soggetti che registrano devono possedere credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza. Laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione. Per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto (utilizzare la sovrascrittura). Nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele: in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini. Qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all´art. 615-ter del codice penale[34]. La trasmissione tramite una rete pubblica

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza. Le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (Es. WI-FI).

Per i diritti degli interessati (pazienti e personale interno dello Studio) vale quanto esposto al punto 3.

È necessario sottolineare che lo Studio medico e odontoiatrico, a meno che non vi operi un singolo medico o un singolo odontoiatra, è un luogo di lavoro. Come tale si applica quanto disposto dal 4.1 del Provvedimento Generale e dallo Statuto dei Lavoratori (L. 300/1970). In particolare, con la videosorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa; è vietata, quindi, l'installazione di apparecchiature specificatamente preordinate alla predetta finalità. Non devono essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa. Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell´art. 4 della Legge 300/1970 (modificata dal D. Lgs. 151/2015), gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. […] In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro […]. Siccome la quasi totalità degli Studi non dispone di rappresentanza sindacale, il titolare dello Studio deve necessariamente inoltrare un'istanza[35] dinanzi l'Ispettorato del lavoro prima che installi l'impianto di videosorveglianza. Importante: non è ammissibile il consenso dei dipendenti/lavoratori all'installazione dell'impianto di videosorveglianza in alternativa alla procedura dinanzi l'Ispettorato del lavoro.[36]

Infine, non bisogna dimenticare che anche in ambito Videosorveglianza trovano largo spazio il Registro dei Trattamenti e la Valutazione di Impatto, trattate nei punti 8 e 9. Nel Registro dello Studio dovrà essere inserita un'apposita riga per il trattamento dati Videosorveglianza; mentre bisognerà condurre una Valutazione di Impatto per tutti quei trattamenti dati Videosorveglianza che possano essere un rischio per i diritti e le libertà delle persone fisiche. Non ci si dimentichi, inoltre, l'art. 35.3 c) GDPR, che obbliga la conduzione di una Valutazione di Impatto in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico (caso tipico di videosorveglianza, ma su larga scala, concetto già esaminato al punto 9).

Considerazioni conclusive

A conclusione di questo articolo, una raccomandazione: è necessario che lo Studio medico e odontoiatrico adotti un "cambio di rotta", dal vecchio regime formale al nuovo regime sostanziale. La protezione dei dati personali è cambiata, e tutto gira attorno alla responsabilità del Titolare e al suo "dovere" di dar conto di ogni sua scelta.

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

Quindi, l'importante è fare presto e adeguarsi il prima possibile, anche per evitare di incorrere nelle sanzioni/risarcimenti di cui al punto precedente.

NOTE

1. In lingua inglese i concetti di "Accountability" e "Responsibility" sono diversi. La differenza maggiore sta nella "condivisione": la Responsibility può essere condivisa, l'Accountability no. Essere "Accountable" significa non solo essere "Responsible" per qualcosa, ma significa anche rispondere delle proprie azioni. Nella versione inglese del GDPR è presente la parola "Accountability", tradotta in italiano con Responsabilizzazione. Ma, in ogni caso, si devono intendere similarmente.
2. Autorità amministrativa indipendente che si occupa di tutti gli ambiti, pubblici e privati, nei quali occorre assicurare il corretto trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle informazioni personali. https://www.garanteprivacy.it/web/guest/home/autorita/compiti.
3. Ai fini di questo articolo si utilizza il termine "Informativa/e" in luogo di "Informazioni" per la maggiore diffusione del vecchio termine nel linguaggio comune, anche tra i professionisti sanitari. Raccomandazione: nei documenti di Studio utilizzare sempre il termine "Informazioni".
4. Ai fini di questo articolo si fa riferimento all'art. 13 GDPR (Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato), in quanto nella quasi totalità dei casi la raccolta di dati personali da parte dello Studio avviene direttamente presso l'interessato.
5. Per approfondimenti: https://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e intenazionale/trasferimento-dei-dati-verso-paesi-terzi
6. […] le finalità del trattamento; le categorie di dati personali in questione; i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; il diritto di proporre reclamo a un'autorità di controllo; qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; l'esistenza di un processo decisionale automatizzato […]
7. Per approfondimenti sul Diritto alla Cancellazione dei dati: https://www.agendadigitale.eu/sicurezza/il-diritto-alloblio/
8. Per approfondimenti sul Diritto alla Portabilità dei Dati: https://www.agendadigitale.eu/sicurezza/portabilita-dei-dati-nel-gdpr-cosa-significa-e-cosa-implica-questo-nuovo-diritto/

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

9. Con il GDPR per dati particolari si intendono gli "ex" dati sensibili di cui al vecchio Codice Privacy.
10. Si veda anche: https://www.agendadigitale.eu/sicurezza/gdpr-cose-legittimo-interesse-si-applica-al-marketing-diretto/
11. Si veda anche: https://www.garanteprivacy.it/regolamentoue/fondamenti-di-liceita-del-trattamento
12. Tecnica che permette di conservare i dati personali in una forma che impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive.
13. Tecnica che permette di offuscare il dato personale, in modo da non essere comprensibile o intelligibile a persone non autorizzate a trattarlo.
14. Il backup è la duplicazione di un file o di un insieme di dati su un supporto esterno al computer, per avere una copia di riserva; il disaster recovery è l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture, a fronte di gravi emergenze che ne intacchino la regolare attività.
15. Si veda: https://www.garanteprivacy.it/regolamentoue/databreach
16. Per maggiori informazioni sulla notifica di un Data Breach al Garante Privacy si veda: https://www.agendadigitale.eu/sicurezza/data-breach-nel-gdpr-cose-e-cosa-sapere-per-segnalazione-e-prevenzione/
17. Novellato dal D.Lgs. 101/2018, in vigore dal 19/09/2018 http://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg
18. Per approfondimenti: https://www.agendadigitale.eu/sicurezza/privacy/gdpr-come-devono-cambiare-i-rapporti-contrattuali-tra-titolare-e-responsabile-trattamento-dati/ e https://www.agendadigitale.eu/sicurezza/privacy/gdpr-chi-e-responsabile-di-cosa-chiariamo-i-dubbi-diffusi-tra-le-aziende/
19. Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248) – https://www.garanteprivacy.it/regolamentoue/DPIA
20. Dal 25 maggio 2018 il WP29 è diventato Comitato Europeo per la Protezione dei Dati – https://edpb.europa.eu/about-edpb/about-edpb_it
21. Si veda: https://www.garanteprivacy.it/regolamentoue/DPIA#STRUMENTI
22. Per approfondimenti sulla Valutazione d'Impatto: https://www.agendadigitale.eu/sicurezza/data-protection-ecco-cosa-cambia-con-le-linee-guida-sulla-dpia/
23. Per approfondimenti sulla figura del DPO: https://www.agendadigitale.eu/sicurezza/privacy/privacy-cos-e-e-come-scegliere-il-data-protection-officer/
24. Si veda anche la recente sentenza TAR Friuli Venezia Giulia sul DPO: http://www.dirittoegiustizia.it/allegati/16/0000082282/TAR_Friuli_Venezia_Giulia_sez_I_sentenza_n_287_18_depositata_il_13_settembre.html
25. Si veda: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5306161
26. Si veda: http://europa.eu/rapid/press-release_IP-18-4501_it.htm
27. Per approfondimenti: https://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi
28. Per maggiori dettagli: https://www.garanteprivacy.it/cookie

GDPR per lo studio medico e odontoiatrico: la guida per gli adempimenti

29. CGUE – Sentenza del 5 giugno 2018 (Causa C-210/16) – http://curia.europa.eu/juris/liste.jsf?num=C-210/16
30. Si veda, tra tutte: https://blog.eset.it/2017/01/la-vulnerabilita-della-crittografia-end-to-end-di-whatsapp/
31. Si veda il caso britannico: https://www.healthcareitnews.com/news/facebook-messenger-whatsapp-imessage-use-uk-nhs-adds-new-security-concerns
32. https://www.ordinedeimedici.cb.it/comunicazione/comunicazioni-ordine/la-deontologia-ai-tempi-di-facebook/
33. Si veda: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680
34. Art. 615-ter. – Accesso abusivo ad un sistema informatico o telematico.Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.La pena è della reclusione da uno a cinque anni:
    1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
    2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesamente armato;
    3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

    Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

    Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio. ↑
35. Di seguito il modello utilizzabile per esperire l'istanza dinanzi l'Ispettorato del lavoro (si noti ancora il rimando al "defunto" art. 13 del D. Lgs. 196/2003): https://www.ispettorato.gov.it/it-it/strumenti-e-servizi/Modulistica/Documents/Autorizzazione%20installazione%20di%20impianti%20di%20videosorveglianza%20o%20GPS/Istanza-videosorveglianza-impianti-audiovisivi.pdf
36. Cass. Pen. Sez. 3, n. 38882 e 38884 del 24 agosto 2018.