GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

Che cos'è il GDPR?

Per "GDPR" ("General Data Protection Regulation") si intende il nuovo Regolamento Europeo n. 679/2016 in materia di protezione dei dati personali. La nuova normativa entrerà pienamente in vigore in tutti i Paesi dell'Unione Europea il prossimo 25 maggio 2018.

Privacy e Codice Deontologico

L’obbligo del medico di mantenere la più assoluta riservatezza su tutto ciò che egli viene a conoscenza sui propri pazienti in virtù del suo ruolo professionale è certamente un obbligo morale che deriva dall’etica deontologica codificata dall’art.10 del Codice Deontologico: ***Segreto professionale “Il medico deve mantenere il segreto su tutto ciò che gli è confidato o di cui venga a conoscenza nell’esercizio della professione”***

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

Privacy

La protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, è **un diritto fondamentale**. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza.

Il regolamento nasce dalla constatazione della crescente pervasività dei servizi digitali e della digitalizzazione in generale. Tali servizi hanno aumentato a dismisura l'esposizione verso il mondo esterno dei dati personali di ogni soggetto privato e la quantità di informazioni ricavabili in termini comportamentali.

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

Come faccio a sapere se il GDPR si applica alla mia attività?

Qualsiasi azienda o professionista che tratta dati personali in Italia o in un altro Paese dell'Unione Europea, è tenuto ad adeguarsi al GDPR. Il GDPR si applica anche a imprese ed enti che hanno sede al di fuori dell'Unione Europea, ad esempio se vendono beni o servizi, anche via internet, all'interno dell'Unione Europea.

Ma che cos'è un dato personale?

In pratica, un dato personale è qualunque informazione riconducibile ad un individuo. Ad esempio, sono dati personali il nome e cognome di una persona e tutti i suoi dati anagrafici, l'indirizzo e-mail, il numero di telefono, ma anche una fotografia, i suoi dati biometrici (es. l'impronta digitale o le caratteristiche della sua firma autografa), il suono della sua voce, le sue abitudini alimentari. Alcune categorie di dati (come quelli relativi ai dati genetici, allo stato di salute, all'orientamento sessuale o all'apparenza a partiti e sindacati) sono considerati **sensibili** e richiedono misure aggiuntive di protezione in base alla normativa.

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

In quali situazioni il GDPR non si applica?

Il regolamento europeo privacy non si applica a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale. Il presente regolamento non si applica al trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività relative alla politica estera e di sicurezza comune dell'Unione.

Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

Quali sono le mie responsabilità come azienda o studio e cosa rischio?

Il GDPR definisce nuove regole e - attraverso il principio della **responsabilizzazione (*accountability)*** - impone, a Titolari e Responsabili del trattamento, l’obbligo di adottare comportamenti proattivi volti a prevenire qualsivoglia violazione del diritto alla riservatezza.

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

Ma in pratica cosa si dovrà fare per essere in regola con il GDPR?

Ai sensi del GDPR, si dovranno adottare tutte le misure di protezione dei dati previste dalla normativa.

1. **Analisi dei rischi relativi al trattamento e misure di accontaubility.**
2. **Informativa da rendere all'interessato.**
3. **Raccolta del consenso al trattamento dei dati.**
4. **Modalità del trattamento.**
5. **Nomina degli «incaricati».**
6. **Formazione dei soggetti che effettuano il trattamento.**
7. **Adozione delle misure minime di sicurezza.**
8. **Diritti dell’interessato.**

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

1. **Analisi dei rischi relativi al trattamento e misure di accontaubility.**

Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'**adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento**. Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni **criteri specifici** indicati nel regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese **"data protection by default and by design"** *(art. 25)*, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei **rischi** per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili.**

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

Il secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari è il **Dpia** (Data protection impact assessment o valutazione d'impatto sulla protezione dei dati) ed è relativo al **rischio inerente al trattamento**. Quest'ultimo è da intendersi come **rischio** di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35-36) tenendo conto dei **rischi** noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali **rischi.** All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il **rischio**).

Da qui ne consegue la necessità che ogni titolare disponga di un ***Registro dei trattamenti***

L'elencazione sistematica di tutti i trattamenti dei dati personali effettuati dal professionista con indicazione dei principali elementi di dettaglio atti a identificarli.

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

Registro dei trattamenti

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare 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;
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.

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

2. Informativa da rendere all'interessato.

Il titolare **DEVE SEMPRE** specificare la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti**.

Il regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

Modalità dell’informativa

Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**.

L'informativa è data, **in linea di principio, per iscritto** e **preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online, siti on line), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra.

Informativa singola per ogni paziente o informativa unica da affiggere in bacheca?

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

Informativa sulla privacy ai sensi del Regolamento Europeo 2016/679

Caro Assistito,

desidero informarTi che in attuazione del Regolamento Europeo 2016/679 **il titolare del trattamento** dei dati personali degli assistiti è

Dr./ssa _____, Cod. Reg. _____,

via _____,

Città _____, Tel._____, Cell. _____.

Ai sensi dell'articolo 13 del RE 2016/679, Ti informo che:

I dati da Te forniti sono trattati nel Tuo interesse per perseguire attività di prevenzione, diagnosi, cura e riabilitazione a tutela della salute e della incolumità fisica, anche in osservanza del Codice Deontologico e del segreto professionale. In conformità ai requisiti di sicurezza richiesti dalla legge, il trattamento sarà effettuato tramite sistemi informatici. Inoltre, tale trattamento, potrà essere esteso con materiale cartaceo e di diagnostica strumentale per immagini.

Particolari trattamenti, come quelli per la medicina di gruppo, la medicina in rete, la ricerca scientifica e la sperimentazione clinica controllata di medicinali, in conformità alle leggi e ai regolamenti, la teleassistenza, la telemedicina e quelli per fornirti altri beni e servizi nel Tuo interesse, potrebbero richiedere l'utilizzo di sistemi di trasmissione dati e reti di comunicazione elettronica, la cui sicurezza non è gestita dal titolare del trattamento;

In ottemperanza a disposizioni di legge, i dati della ricettazione così come i certificati di malattia saranno trasmessi per via telematica ai vari soggetti individuati dal legislatore, soggetti che assumono il ruolo di titolari della sicurezza dei loro sistemi.

Il conferimento dei dati è facoltativo;

Un eventuale rifiuto di consentire il trattamento di tali dati potrebbe comportare l'impossibilità di prosecuzione del rapporto poiché verrebbe a mancare il perseguimento delle attività di cui al comma a);

Il trattamento riguarda anche e soprattutto dati personali denominati "sensibili", vale a dire dati idonei a rivelare lo stato di salute e la vita sessuale. I dati non saranno oggetto di diffusione.

Possono, però essere consultati dai medici da me incaricati per la sostituzione in caso di mia assenza, e dalla segretaria per l'aggiornamento e la manutenzione del diario visite; inoltre, possono essere trattati da altri medici da me designati nelle modalità previste dalla medicina di gruppo e/o dalla medicina in rete.

Potranno, qualora ciò sia necessario per erogare una prestazione e/o un servizio nel Tuo interesse, essere comunicati a:

organismi sanitari pubblici (asl, ospedali, etc);

organismi sanitari privati (cliniche, laboratori di analisi, etc.) ed esercenti le professioni sanitarie (medici specialisti, farmacisti, etc.);

enti di assistenza e previdenza (Inps, Inail, etc.);

limitatamente a quei dati ed operazioni indispensabili per perseguire le finalità di cui al comma a).

I dati sanitari potranno essere trattati da centri medici specializzati nel valutare l'idoneità al lavoro.

Infine, **per l'eventuale comunicazione di tali dati a Tuoi familiari, devi, preventivamente ed ogni qualvolta ciò sia necessario, autorizzare per atto scritto il/i familiare/i da Te designato/i alla ricezione di tale comunicazione;**

Inoltre i Tuoi dati anagrafici potranno essere comunicati al Consulente Commercialista per la registrazione della documentazione fiscale.

Il personale addetto all'assistenza e manutenzione dei sistemi informatici utilizzati potrebbe avere accesso ai tuoi dati sensibili.

In ogni momento potrai esercitare i Tuoi diritti nei confronti del titolare del trattamento e precisamente potrai chiedere l'accesso ai tuoi dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento o l'opposizione al trattamento. Potrai esercitare tali diritti inviando una comunicazione scritta al titolare. Inoltre hai diritto di proporre reclamo al Garante per la protezione dei dati personali secondo le modalità fornite in http://www.garanteprivacy.it/web/guest/home/modulistica

I dati personali non saranno trasferiti ad un paese terzo né ad una organizzazione internazionale.

I dati saranno conservati per 10 anni dopo revoca del consenso o dopo la cessazione del rapporto di cura.

Lì, ……

…….

firma

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

3. Raccolta del consenso al trattamento dei dati.

Per I trattamento di dati **"sensibili"** il consenso **DEVE** essere **"esplicito";** lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati.

- **NON** deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso; inoltre, il titolare **DEVE** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.
- Il **consenso dei minori** è valido **a partire dai 16 anni** (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci. Quando l'assistito raggiunge la maggiore età, il consenso deve essere rinnovato con una nuova prestazione.
- **DEVE** essere, in tutti i casi, libero, specifico, informato e inequivocabile e **NON** è ammesso il consenso tacito o presunto (no a caselle prespuntate su un modulo).
- Una volta compilato dall'interessato, deve essere conservato in un luogo il cui accesso sia consentito solo alle persone autorizzate al trattamento dei dati.

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

RACCOMANDAZIONI

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.

In particolare, occorre verificare che la richiesta di consenso sia **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2).

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

MODULO CONSENSO INFORMATO (REGOLAMENTO EUROPEO 2016/679)
Io sottoscritto**: .....,** Nato a **.....,** il …… Residente a …….**.....**
Assistito del dr. **……..,** dallo stesso informato su:
la necessità di raccogliere i dati anagrafici e personali riferiti alle mie condizioni di salute;
il fatto che tali informazioni verranno trattate con strumenti elettronici per finalità connesse alle attività di prevenzione, diagnosi, cura e riabilitazione a tutela della mia salute;
il trattamento dei dati personali per scopi scientifici (ricerca scientifica e/o sperimentazione clinica controllata di medicinali), nell'ambito della teleassistenza o telemedicina, per fornire altri beni e servizi attraverso una rete di comunicazione elettronica;
i dati della ricettazione e i certificati di malattia, in ottemperanza a disposizione di legge, saranno inviati per via telematica ai diversi soggetti individuati dal legislatore, soggetti che diventano i titolari della sicurezza dei loro sistemi;
la possibilità che tali informazioni siano disponibili per la consultazione da medici da me incaricati per la sostituzione in caso di mia assenza, e dalla segretaria per l'aggiornamento e la manutenzione del diario visite, nonché dai medici in associazione.
la possibilità che i Tuoi dati anagrafici potranno essere comunicati al Consulente Commercialista per la registrazione della documentazione fiscale.
la possibilità che tali informazioni potranno essere fornite in forma anonima a terzi per effettuare ricerche epidemiologiche ed analisi statistiche; tali informazioni potranno essere rielaborate, in forma aggregata e anonima e quindi senza nessun riferimento alle persone.
la possibilità che i dati possono essere visionati dal personale incaricato dell'assistenza e manutenzione dei sistemi informatici.
i dati, qualora sia necessario per erogare una prestazione e/o un servizio nel Tuo interesse, potranno essere comunicati a:
organismi sanitari pubblici (asl, ospedali, etc);
organismi sanitari privati (cliniche, laboratori di analisi, etc.) o esercenti le professioni sanitarie (medici specialisti, farmacisti, personale dell'ADI etc.);
enti di assistenza e previdenza (Inps, Inail, etc.);
limitatamente a quei dati ed operazioni indispensabili per perseguire le finalità di cui al comma 1).
la possibilità che i dati informatici in suo possesso verranno trattati da terzi per la sincronizzazione degli stessi da/verso un unico Data Center, anche con il sistema del CLOUD COMPUTING, per rendere possibile l'interscambio della cartella con i colleghi della medicina in rete, durante la visita ambulatoriale;
11. le misure atte a garantire la riservatezza delle informazioni;

ESPRIMO IL MIO CONSENSO E AUTORIZZO
Il dr. **……** i medici sostituti e in associazione, nonché eventuali collaboratori da lui autorizzati.
Tale consenso è esteso anche a gruppi di cura esterni (Specialisti, reparti ospedalieri, Emergenza) attivati dal
dr. **……..**
Inoltre Io sottoscritto autorizzo il titolare del trattamento e i soggetti abilitati al trattamento, secondo le rispettive competenze, a consegnare la documentazione sanitaria alle persone da me delegate e sottoindicate:
……
……

FIRMA

……..
Letta l'informativa nego il mio consenso per:
* tutto quanto in premessa: .....
* solo per i seguenti punti: .....
FIRMA

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

MODULO CONSENSO INFORMATO (REGOLAMENTO EUROPEO 2016/679) x MINORI
Io sottoscritto**: ……………………………………………………………………………, Nato a ………………………………………….., il** ……………… Residente a ………..**…………………………………………….., Genitore di ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,….,,,**
Assistito del dr. **………………………………………,** dallo stesso informato su:
la necessità di raccogliere i dati anagrafici e personali riferiti alle mie condizioni di salute;
il fatto che tali informazioni verranno trattate con strumenti elettronici per finalità connesse alle attività di prevenzione, diagnosi, cura e riabilitazione a tutela della mia salute;
il trattamento dei dati personali per scopi scientifici (ricerca scientifica e/o sperimentazione clinica controllata di medicinali), nell'ambito della teleassistenza o telemedicina, per fornire altri beni e servizi attraverso una rete di comunicazione elettronica;
i dati della ricettazione e i certificati di malattia, in ottemperanza a disposizione di legge, saranno inviati per via telematica ai diversi soggetti individuati dal legislatore, soggetti che diventano i titolari della sicurezza dei loro sistemi;
la possibilità che tali informazioni siano disponibili per la consultazione da medici da me incaricati per la sostituzione in caso di mia assenza, e dalla segretaria per l'aggiornamento e la manutenzione del diario visite, nonché dai medici in associazione.
la possibilità che i Tuoi dati anagrafici potranno essere comunicati al Consulente Commercialista per la registrazione della documentazione fiscale.
la possibilità che tali informazioni potranno essere fornite in forma anonima a terzi per effettuare ricerche epidemiologiche ed analisi statistiche; tali informazioni potranno essere rielaborate, in forma aggregata e anonima e quindi senza nessun riferimento alle persone.
la possibilità che i dati possono essere visionati dal personale incaricato dell'assistenza e manutenzione dei sistemi informatici.
i dati, qualora sia necessario per erogare una prestazione e/o un servizio nel Tuo interesse, potranno essere comunicati a:
organismi sanitari pubblici (asl, ospedali, etc);
organismi sanitari privati (cliniche, laboratori di analisi, etc.) o esercenti le professioni sanitarie (medici specialisti, farmacisti, personale dell'ADI etc.);
enti di assistenza e previdenza (Inps, Inail, etc.);
limitatamente a quei dati ed operazioni indispensabili per perseguire le finalità di cui al comma 1).
la possibilità che i dati informatici in suo possesso verranno trattati da terzi per la sincronizzazione degli stessi da/verso un unico Data Center, anche con il sistema del CLOUD COMPUTING, per rendere possibile l'interscambio della cartella con i colleghi della medicina in rete, durante la visita ambulatoriale;
11. le misure atte a garantire la riservatezza delle informazioni;
ESPRIMO IL MIO CONSENSO E AUTORIZZO
Il dr. **……………………………………** i medici sostituti e in associazione, nonché eventuali collaboratori da lui autorizzati.
Tale consenso è esteso anche a gruppi di cura esterni (Specialisti, reparti ospedalieri, Emergenza) attivati dal dr. **……………………………………….**
Inoltre Io sottoscritto autorizzo il titolare del trattamento e i soggetti abilitati al trattamento, secondo le rispettive competenze, a consegnare la documentazione sanitaria alle persone da me delegate e sottoindicate:
…………………………………………………………………………………………….
…………………………………………………………………………………………….

FIRMA

…………………………………..
Letta l'informativa nego il mio consenso per:
* tutto quanto in premessa: ....
* solo per i seguenti punti: ....
FIRMA
…………………………………

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

4. Modalità del trattamento.

In **premessa** è necessario ricordare che la tenuta e l'aggiornamento di una scheda sanitaria individuale per ciascuno dei propri pazienti rientra tra i compiti del medico di medicina generale e del pediatra di libera scelta.
Infatti gli Accordi Collettivi Nazionali all'art. 45 (Medicina Generale) e all'art. 44 (Pediatria di Libera Scelta*) (Compiti del medico),* precisa al comma 2 che: ***"L'espletamento delle funzioni di cui al precedente comma 1 (cioè "funzioni e compiti individuali del medico di assistenza primaria e del pediatra di libera scelta") si realizza con:***
b) la tenuta e l'aggiornamento di una scheda sanitaria individuale, su supporto informatico, ad uso del medico e ad utilità dell'assistito e del SSN, secondo standard nazionali e regionali e modalità definite nell'ambito degli Accordi regionali".

La scheda sanitaria da mero supporto alla memoria del professionista (e dunque destinato al suo esclusivo o prevalente impiego, previsto dai precedenti ACN) diventa ***un documento che assume i caratteri della ufficialità e della finalità alla consultazione da parte di terzi, nonché della condivisione delle informazioni nell'ottica del bene del paziente e della continuità e coerenza delle cure.***

Da ciò deriva che essendo un documento contenente dati sanitari ***"sensibili"*** il titolare del trattamento, cioè il medico di medicina generale o il pediatra di libera scelta, doveva ottemperare a tutto quanto previsto dal Codice privacy (D.Lgs 196/2003) e ora dal GDPR (2016/679) se non vuole incorrere in spiacevoli conseguenze civili e penali.

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

4. Modalità del trattamento.

AUTORIZZAZIONE PER MEDICI – COLLABORATORI
ARCHIVI ELETTRONICI

Il/La sottoscritto/a Dr./Dott.ssa

Cognome _____, Nome _____
Nato a _____, il _____ e Residente a _____
Via/P.zza _____, n° _____, con studio medico in Via/P.zza _____, n° _____, Città _____, Codice Regionale _____, MMG |_| - PLG |_|
Titolare del Trattamento dei dati ai sensi e per gli effetti dell'art. 24 del R.EU 2016/679, ai fini dell'applicazione della normativa vigente, adotta le seguenti disposizioni:

1. **Nomina del "Responsabile del trattamento" art. 28 R.EU 2016/679**
2. **Nomina delle "Persone autorizzate al trattamento": Medici sostituti Collaboratore di studio, Infermiere di studio, Consulente informatico, Consulente commercialista, Consulente del lavoro, Medici dell'associazione di gruppo o Medici dell'associazione in rete, Medici Tirocinanti.**
3. **Personale non sanitario con accesso allo studio**

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

ATTO DI AUTORIZZAZIONE INCARICATO (COLLABORATORE DI STUDIO-INFERMIERE)

Spett.le

OGGETTO: nomina della sua persona quale incaricato per il trattamento dei dati personali .

In relazione al rapporto di lavoro (COLLABORATORE di STUDIO/ INFERMIERE di STUDIO) con Lei in essere, con la presente Le affidiamo il trattamento di dati personali nell'ambito delle funzioni che è chiamato/a a svolgere presso la nostra struttura.

A tal fine vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

il trattamento dei dati deve essere effettuato in modo lecito e corretto;

i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;

è necessaria una verifica costante dei dati e il loro aggiornamento;

è necessaria la verifica costante della completezza e pertinenza dei dati trattati;

devono essere rispettate le misure di sicurezza previste dal R.EU. 2016/679.

Per ogni operazione del trattamento deve essere garantita la massima riservatezza e in particolare:

divieto di comunicazione o diffusione dei dati senza la preventiva autorizzazione del Titolare/Responsabile;

l'accesso dei dati è autorizzato limitatamente all'espletamento delle proprie funzioni;

in caso di interruzione, anche temporanea, del lavoro verificare che i dati non siano accessibili a terzi non autorizzati.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione dell'incarico.

Trattamento consentito:

raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli dell'azienda e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo per soggetti autorizzati;

qualsiasi altra operazione di trattamento nei limiti del mandato ricevuto e nel rispetto delle norme di legge;

divieto di comunicazione a terzi se non per ragioni strettamente legate all'incarico, con nostra espressa autorizzazione o per ragioni imposte da norme legislative.

Il trattamento operato riguarda il trattamento dei dati come di seguito specificato:

Accede ai dati anagrafici e ai dati sensibili dei pazienti afferenti lo studio in attività di supporto al titolare

Si precisa che gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto sono da lei dovuti in base al contratto di lavoro

Distinti Saluti,

Firma del titolare

Per accettazione , lì …… ……..

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

ATTO DI AUTORIZZAZIONE INCARICATO (CONSULENTE INFORMATICO COMMERCIALISTA, DEL LAVORO)

SPETT.le
OGGETTO: nomina della sua persona quale incaricato per il trattamento dei dati importanti e/o sensibili .
In relazione al rapporto di lavoro con Lei in essere, con la presente Le affidiamo il trattamento di dati personali nell'ambito delle funzioni che è chiamato/a a svolgere presso la nostra struttura.
A tal fine vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:
il trattamento dei dati deve essere effettuato in modo lecito e corretto;
i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
è necessaria una verifica costante dei dati e il loro aggiornamento;
è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
devono essere rispettate le misure di sicurezza previste dal R.EU. 2016/679.
Per ogni operazione del trattamento deve essere garantita la massima riservatezza e in particolare:
divieto di comunicazione o diffusione dei dati senza la preventiva autorizzazione del Titolare;
l'accesso dei dati è autorizzato limitatamente all'espletamento delle proprie funzioni;
in caso di interruzione, anche temporanea, del lavoro verificare che i dati non siano accessibili a terzi non autorizzati;
il personale che utilizzerete e che verrà a conoscenza dei dati dovrà essere formato e rispettare tutte le misure di sicurezza imposte dalla legge.
Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione dell'incarico. Per ogni altra misura qui non prevista si fa riferimento al documento programmatico sulla sicurezza adottata dall'azienda.
Trattamento consentito:
raccogliere ,registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli dell'azienda e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo per soggetti autorizzati;
qualsiasi altra operazione di trattamento nei limiti del mandato ricevuto e nel rispetto delle norme di legge;
divieto di comunicazione a terzi se non per ragioni strettamente legate all'incarico, con nostra espressa autorizzazione o per ragioni imposte da norme legislative.

Il trattamento operato riguarda il trattamento dei dati come di seguito specificato:
Accede ai dati economici, fiscali e del personale e dei consulenti (Sensibili limitatamente alle anagrafiche) nell'ambito delle funzioni di Consulente Commercialista
Distinti Saluti,

Firma del Titolare

Per accettazione
lì …… ……. ……

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

ATTO DI AUTORIZZAZIONE INCARICATO (Medico sostituto, Medici dell'associazione, Medico tirocinante del CFSMG)
SPETT. dr.
OGGETTO: nomina della sua persona quale contitolare per il trattamento dei dati personali .
In relazione al rapporto professionale con Lei in essere, con la presente Le affidiamo il trattamento di dati personali nell'ambito delle funzioni che è chiamato/a a svolgere presso la nostra struttura.
A tal fine vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:
il trattamento dei dati deve essere effettuato in modo lecito e corretto;
i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
è necessaria una verifica costante dei dati e il loro aggiornamento;
è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
devono essere rispettate le misure di sicurezza previste dal R.EU. 2016/679.
Per ogni operazione del trattamento deve essere garantita la massima riservatezza e in particolare:
divieto di comunicazione o diffusione dei dati senza la preventiva autorizzazione del Titolare/Responsabile;
l'accesso dei dati è autorizzato limitatamente all'espletamento delle proprie funzioni;
in caso di interruzione, anche temporanea, del lavoro verificare che i dati non siano accessibili a terzi non autorizzati.
Gli obblighi relativi alla riservatezza , alla comunicazione ed alla diffusione dei dati dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione dell'incarico. Per ogni altra misura qui non prevista si fa riferimento al documento programmatico sulla sicurezza adottata dall'azienda.
Trattamento consentito:
raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli dell'azienda e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo per soggetti autorizzati;
qualsiasi altra operazione di trattamento nei limiti del mandato ricevuto e nel rispetto delle norme di legge;
divieto di comunicazione a terzi se non per ragioni strettamente legate all'incarico, con nostra espressa autorizzazione o per ragioni imposte da norme legislative.

Il trattamento operato riguarda il trattamento dei dati come di seguito specificato:
Accede ai dati sensibili finalizzato al raggiungimento dello scopo precipuo dell'associazione e/o come medico sostituto in assenza del titolare
Distinti Saluti,

Firma del Titolare

Per accettazione Nome e cognome ……..
, lì …… ----------
Firma del Contitolare

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

Chi è il responsabile della protezione dei dati personali (DPO) e quali sono i suoi compiti?

Il responsabile della protezione dei dati personali è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679. Si tratta di un soggetto designato dal titolare del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità (e proprio per questo, il suo nominativo va comunicato al Garante) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.

Quali requisiti deve possedere il responsabile della protezione dei dati personali?

Il responsabile della protezione dei dati personali, al quale non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi, deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.

Deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici.

Il responsabile della protezione dei dati personali deve poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

Obbligo di Nomina del DPO o RPD (Data Protection Officer o Responsabile del trattamento)

a) se il trattamento è svolto da un’autorità pubblica o da un organismo pubblico;
b) se le attività principali del titolare del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
c) se le attività principali del titolare del trattamento consistono ***nel trattamento su larga scala*** di categorie particolari di dati* o di dati personali* relativi a condanne penali e reati.

* Ai sensi dell’articolo 9, si tratta di dati personali i dati che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose, o l’appartenenza sindacale, oltre al trattamento di dati genetici, dati biometrici al fine dell’identificazione univoca di una persona fisica, e. **di dati relativi alla salute, alla vita sessuale o all’orientamento sessuale di una persona fisica**

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

TRE TIPOLOGIE

1. MMG o PLS che non hanno obbligo di nominare il RPD;

2. MMG o PLS per i quali è consigliabile la nomina del RPD;

3. MMG o PLS per i quali è obbligatoria la nomina del RPD.

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

5. Formazione dei soggetti che effettuano il trattamento.

Per quanto riguarda la Formazione, la normativa non prevede la necessità di acquisire un attestato di avvenuta formazione come ad esempio le questioni sulla sicurezza in ambito lavorativo, ma un "obbligo di conoscenza" per ottenere il quale il Titolare dello studio medico si dovrà attivare affinché siano realizzate tutte quelle iniziative di sua competenza idonee a dimostrare un reale impegno nella acquisizione da parte sua e dei suoi Collaboratori, delle conoscenza delle nuove norme sulla sicurezza dei dati.

Per tali motivi FIMMG Nazionale attraverso APRIFORM, Ente Formativo di ConfProfessioni, provvederà a realizzare i necessari corsi formativi per ottemperare agli obblighi di conoscenza, previsti dal nuovo regolamento. Utilizzando le risorse dei Fondi Bilaterali per la formazione continua (FONDOPROFESSIONI per i Settore degli Studi Professionali), APRIFORM, in totale gratuità realizzerà piani formativi per **i Collaboratori di Studio iscritti a Fondoprofessioni. Ricordiamo che l'iscrizione al Fondo è del tutto gratuita e deve essere fatta una sola volta, annotando la sigla "FPRO" sul modello UNIEMENS (ex DM-10), da parte del consulente del lavoro.**
Per i Titolari di Studio i cui Collaboratori parteciperanno ai Corsi di Formazione APRIFORM, metterà a disposizione un Corso FAD sulla Privacy della durata di 8 ore per la loro formazione personale.

I corsi inizieranno da OTTOBRE 2018 e verrà rilasciata una dichiarazione al momento della avvenuta iscrizione al Corso, per ogni partecipante, affinché ogni Titolare di Studio Medico possa dimostrare l' avvio del processo formativo volto a sviluppare maggiori conoscenze e competenze in ambito di privacy.

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

7. Adozione delle misure minime di sicurezza.

Le misure minime di sicurezza richieste sono tecniche, informatiche, organizzative, logistiche e procedurali; sono tutte orientate a ridurre i rischi che incombono sui dati personali trattati con archivi elettronici.

a. **Registrazione dei dati**: non lasciare incustodita la postazione di lavoro durante la fase di inserimento dei dati, non lasciare chiavette USB, dischetti, fogli, cartelle a disposizione di estranei.
b. **Archiviazione dei dati:** il materiale cartaceo deve essere custodito in armadi, schedari, cassette muniti di serratura. Il personale di studio deve avere cura di evitare che le informazioni trattate possano essere visualizzate e rese conoscibili a terzi.
c. **Sistema di autenticazione informatica**: Ad ogni persona terza incaricata, il titolare deve fornire una parola chiave onde consentire l'accesso all'archivio informatico. La parola chiave è composta da almeno otto caratteri. A riguardo oltre alla password di accesso al programma, è consigliabile anche impostare una password di accesso al computer. Le password vanno rinnovate regolarmente ogni tre mesi.

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

7. Adozione delle misure minime di sicurezza.

d. I dati sensibili devono essere protetti contro il rischio di intrusione **(trojan),** e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale **(malware),** mediante l'attivazione di idonei strumenti elettronici **(antivirus, firewall)** da aggiornare periodicamente.
e. Aggiornamenti periodici dei programmi.
f. I dati devono essere salvati (backup) con frequenza almeno settimanale. Devono essere impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
g. Devono essere adottate idonee misure per garantire il **ripristino dell'accesso dei dati (restore)** in caso di danneggiamento degli stessi o degli strumenti elettronici **(disaster recovery)** in tempi non superiori a sette giorni.
h. Data breach notification

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

7. Adozione delle misure minime di sicurezza. h. Data breach notification

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica (modulistica scaricabile da: http:/www.garanteprivacy.it/web/guest/home/modulistica) deve contenere le seguenti notizie:

- Natura della violazione, le categorie il numero approssimativo di interessati coinvolti, le categorie e quantità di dati violati
- Descrivere le possibili conseguenze della violazione
- Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La notifica all'interessato non è necessaria allorquando:

- La violazione interessa dati cifrati
- Il titolare ha adottato misure (anche successivamente) atte a scongiurare un rischio elevato
- La comunicazione comporta un sforzo sproporzionato

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

8. Diritti dell’interessato.

a. **Modalità di esercizio dei diritti:** Il termine per la risposta all'interessato è, **per tutti i diritti (compreso il diritto di accesso), 1 mese**, estendibili fino a 3 mesi in casi di particolare complessità; **il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.**
   La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche **concisa, trasparente e facilmente accessibile**, oltre a utilizzare un **linguaggio semplice e chiaro**.
b. **Diritto di accesso**. Il diritto di accesso prevede **in ogni caso** il diritto di ricevere **una copia dei dati** personali oggetto di trattamento.
c. **Diritto alla cancellazione (diritto all’oblio):** Il diritto cosiddetto **"all'oblio"** si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati,compresi "qualsiasi link, copia o riproduzione“.

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

8. Diritti dell'interessato.

d. Diritto alla limitazione del trattamento: E' esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare).

- **Diritto alla portabilità dei dati:** Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei). Sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare.
  Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile**.**

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

PROBLEMATICHE APERTE

1. **Utilizzo di internet e posta elettronica:** Il GDPR non affronta in maniera esplicita tali aspetti della quotidianità. Occorre però particolare attenzione alla spedizione con posta elettronica di **file o messaggi contenenti dati sensibili.** In tal caso occorrerà **proteggere il contenuto dei file** dall'accesso e dalla visione di soggetti non autorizzati o non legittimati al trattamento diversi dai destinatari delle comunicazioni elettroniche considerate. E' obbligatorio quindi il ricorso alla **criptazione o cifratura dei messaggi**, in modo da rendere non leggibili i dati in caso di intercettazione delle comunicazioni.
2. **L'uso di CHAT:** Scoraggiare gli assistiti dall'utilizzo di chat per comunicare dati sensibili.
3. **Invio di foto per eventuale consulto:** Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che **consente l'identificazione univoca o l'autenticazione di una persona fisica.**

GDPR: "General Data Protection Regulation" Regolamento Europeo Privacy 2016/679

DPIA: Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio.

STRUMENTI: Un software per la valutazione di impatto

La **CNIL**, l'Autorità francese per la protezione dei dati, ha messo a disposizione un software di ausilio ai titolari in vista della effettuazione della valutazione d'impatto sulla protezione dei dati (DPIA).

Il software - gratuito e liberamente scaricabile dal sito www.cnil.fr (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil) - offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla DPIA.

La **versione in lingua italiana** è stata messa a punto anche con la collaborazione del Garante per la protezione dei dati personali.

GDPR: “General Data Protection Regulation” Regolamento Europeo Privacy 2016/679

GRAZIE PER L’ATTENZIONE