EBOOK DI CONSULCESI CLUB

APP MEDICHE E DATI PERSONALI: GUIDA ALLA GESTIONE PER IL SANITARIO

CONSULCESI CLUB

CONSULCESI CLUB

Formazione ECM, News, Risorse e tool, Elenco Professionisti, Assistenza legale e assicurativa, Sconti e Convenzioni

Tutto in un'unica soluzione digitale innovativa e personalizzabile

CONSULCESI CLUB

INDICE

1. LE APP SANITARIE E IL COMPENDIO DEL GARANTE PRIVACY

È da poco disponibile sul sito del Garante Privacy il Compendio sul trattamento dei dati personali attraverso piattaforme volte a mettere in contatto medici e pazienti attraverso web e app: si tratta di una guida che spiega agli operatori del settore (professionisti sanitari, informatici e aziende sviluppatrici) come devono essere trattati i dati dei pazienti nel caso in cui il contatto tra il medico e il paziente avvenga attraverso un'app o una piattaforma web.

Questo tipo di piattaforme, oramai sempre più diffuse, facilitano sicuramente il contatto tra i pazienti e i professionisti sanitari, tra cui rientrano anche i Medici di Medicina Generale (MMG) e i Pediatri di Libera Scelta, offrendo un'ampia gamma di servizi tra cui la prenotazione di visite specialistiche, la gestione degli appuntamenti, il pagamento delle prestazioni.

Trattandosi di piattaforme dedicate a mettere in contatto tra medico e paziente, è normale che vengano scambiati dei dati sanitari: questi dati non possono essere trattati dai gestori delle piattaforme per scopi di diagnosi o terapia, poiché questo tipo di trattamento può essere effettuato esclusivamente dai professionisti sanitari, i quali – peraltro – sono soggetti al segreto professionale. Le piattaforme potranno trattare esclusivamente i dati necessari per l'erogazione dei servizi, come quelli amministrativi (ad esempio nome e cognome, codice fiscale) o quelli tecnologici.

Il Garante Privacy ha redatto questa guida partendo dal presupposto che solitamente le piattaforme non operano in Italia o in Europa, bensì in paesi terzi, non propriamente attenti alla tutela dei dati personali e sanitari dei cittadini: per questo è richiesto ai titolari delle piattaforme di dimostrare il rispetto dei principi del Regolamento Europeo sulla Privacy (il GDPR), garantendo la tutela dei dati personali fin dalla progettazione dell'app o del sito/piattaforma.

Il documento si propone di identificare gli aspetti principali della protezione dei dati nei servizi digitali che mettono in contatto pazienti e professionisti sanitari.

2. I DATI SULLA SALUTE

Il GDPR definisce i **dati relativi alla salute** come quei dati personali attinenti alla salute fisica o mentale di una persona, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Sono dati relativi alla salute anche **le informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria**, come ad esempio un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco ai fini sanitari.

L'articolo 9 del GPDR vieta, in linea generale, il trattamento dei dati sanitari, salvo che ricorra una delle specifiche esenzioni previste dalla norma:

a. **consenso** del paziente per il trattamento dei dati sanitari per una o più specifiche finalità;
b. necessità di trattare i dati sanitari per **assolvere determinati obblighi o esercitare determinati diritti**, nonché in materia di **diritto del lavoro, sicurezza sociale e protezione sociale**;
c. **tutela di un interesse vitale dell'interessato o di un'altra persona** fisica, qualora **l'interessato si trovi nell'incapacità fisica/giuridica di prestare il proprio consenso**;
d. trattamento effettuato da **fondazioni/associazioni/organismi senza scopo di lucro**;
e. dati **resi pubblici dall'interessato**;
f. necessità di **accertare, esercitare o difendere un diritto davanti a un'autorità giudiziaria**;
g. **motivi di interesse pubblico** (ad esempio un'emergenza derivante da un'epidemia o pandemia, oppure da un sisma o da un'emergenza alimentare);
h. **finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza, terapia sanitaria o sociale, gestione di sistemi e servizi sanitari o sociali** (la c.d. finalità di cura);
i. **motivi di interesse pubblico nel settore della sanità pubblica**;
j. necessità di trattare i dati per **fini di archiviazione o di ricerca scientifica o storica**.

3. DATI SANITARI, PIATTAFORME WEB E APP: LE FINALITÀ ALLA BASE DEL TRATTAMENTO DEI DATI PERSONALI

Secondo l'analisi del Garante lo scopo principale delle piattaforme e delle app sanitarie attualmente esistenti è quello di **agevolare il paziente nella scelta del professionista sanitario, facilitando le comunicazioni:** si tratta, perciò, di un servizio amministrativo (una sorta di segretario virtuale) **legato ad una prestazione sanitaria eventuale e futura**.

I possibili trattamenti dei dati effettuati dalle piattaforme/app, perciò, sono i seguenti:

1. **trattamento dei dati degli utenti utilizzati per la creazione dell'account** – questi dati potrebbero anche essere idonei a rivelare il loro stato di salute (ad esempio in base al tipo di prestazione richiesta o alla specializzazione del professionista sanitario). **Questi dati personali possono essere lecitamente trattati dai gestori di piattaforme/app**, perché la finalità è quella di offrire un servizio di carattere amministrativo all'utente/paziente;
2. **trattamento dei dati personali dei professionisti sanitari che si registrano sulla piattaforma per entrare in contatto con i pazienti** – i dati personali, in questo caso, vengono forniti dal professionista sanitario alla piattaforma/app in virtù di un vero e proprio contratto con cui il medico si registra sulla piattaforma per essere messo in contatto con potenziali pazienti;
3. **trattamento di dati sulla salute dei pazienti** – questo tipo di dati è eventuale, perché potrebbe accadere che il paziente scambi con il professionista sanitario, tramite la piattaforma, informazioni o dati sulla sua salute, anziché limitarsi semplicemente alla intermediazione per la prenotazione di una visita; in questo caso i dati sanitari (contenuti ad esempio documenti sanitari, prescrizioni, referti) possono essere trattati **esclusivamente dal professionista sanitario con la finalità di diagnosi e cura e sotto la sua responsabilità**, trattandosi di professionista tenuto al **segreto professionale**, in virtù dell'art. 9 del GDPR.

4. DATI SANITARI, PIATTAFORME WEB E APP: LE BASI GIURIDICHE PER IL TRATTAMENTO DEI DATI

Le piattaforme, per poter trattare i dati personali sopra elencati, devono avere quella che il GDPR definisce una **base giuridica**, cioè una "pezza d'appoggio" normativa che consente loro di avere conoscenza, maneggiare e conservare i dati senza incorrere in illeciti.

Per poter comprendere appieno chi e perché può trattare i dati dei soggetti interessati, è necessario evidenziare che l'utente della piattaforma non sempre diventa paziente del medico, ma può accadere che dopo essersi registrato e aver scambiato una serie di informazioni sulla sua salute con il professionista sanitario, decida di non proseguire e non diventare suo paziente; per questo motivo il Garante distingue tra i dati sulla salute degli utenti e quelli sulla salute dei pazienti.

I **dati sulla salute degli utenti** che utilizzano una piattaforma/app per prenotare una prestazione (visita, esame strumentale) con un professionista sanitario **non possono essere trattati dal gestore dell'app/piattaforma**, bensì solo dal professionista sanitario, sulla base del preventivo consenso informato dell'utente/paziente; il consenso deve essere:

- **libero**, cioè acquisito liberamente e non estorto,
- **specifico**, vale a dire riferito a quei determinati dati sanitari per le specifiche finalità indicate nell'informativa dall'odontoiatra,
- **informato**, cioè preceduto dalla messa a disposizione, lettura e consegna dell'informativa sul trattamento dei dati personali,
- **inequivocabile**, vale a dire chiaro e indubbio,
- **revocabile** in qualsiasi momento con modalità chiare e semplici di esercizio di tale diritto.

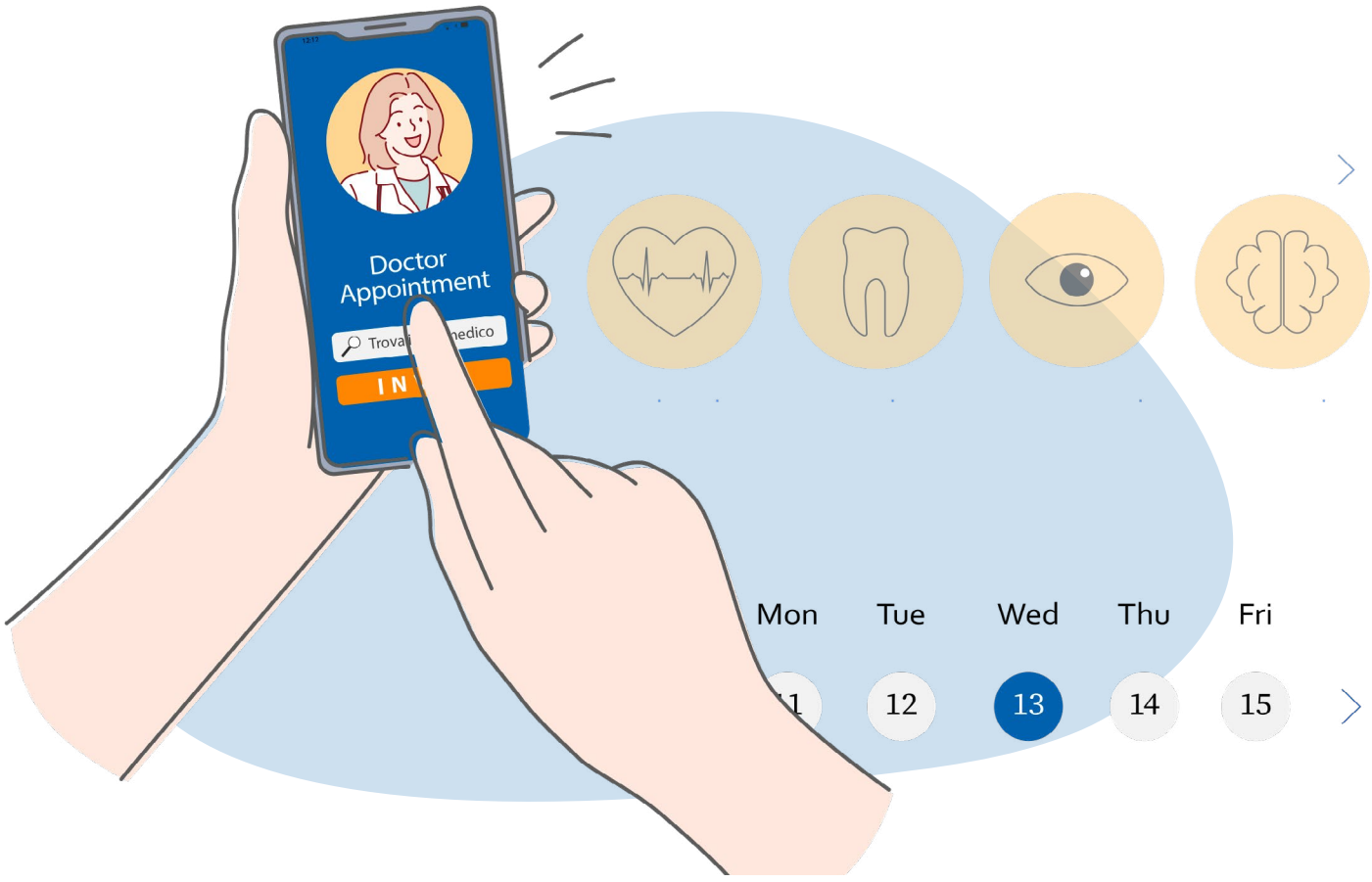
I gestori di app/piattaforme, invece, **non possono trattare i dati sanitari degli utenti**, bensì solo quelli personali (ad esempio nome, cognome, indirizzo, e-mail) che sono necessari per effettuare la prestazione amministrativa di intermediazione nella prenotazione delle visite.

Se la piattaforma ha **ulteriori finalità** oltre quella di fornire la prestazione, come ad esempio **l'invio di comunicazioni commerciali e di marketing su ulteriori servizi offerti dai soggetti proprietari/gestori delle piatta-**

forme, è necessario che l'utente esprima il **consenso per ciascuna di tali finalità "ulteriori"**; ovviamente, il modulo sull'app/piattaforma dovrà essere predisposto in modo tale da consentire all'utente/paziente di negare questo consenso.

La base giuridica che consente ai gestori di app/piattaforme di trattare i **dati personali dei professionisti sanitari** che si registrano sul sito per chiedere di usufruire dei loro servizi è rappresentata dal **contratto di servizi** che si instaura tra questi due soggetti al momento della registrazione.

Il trattamento dei dati sulla salute dei pazienti è vietato ai gestori dell'app/piattaforma ed è esclusivamente riservato al professionista sanitario, il quale ne viene a conoscenza per finalità di diagnosi e cura ed è tenuto al segreto professionale; in virtù della normativa vigente, il professionista sanitario non necessita di ulteriore consenso del paziente per trattare questo tipo di dati, essendo sufficiente, come base giuridica per il trattamento, la norma del GDPR (art. 9).



5. IL DIVIETO DI DIFFONDERE E COMUNICARE I DATI A TERZI

Il GDPR **vieta la diffusione o comunicazione dei dati sullo stato di salute di un soggetto a un terzo**, a meno che non vi sia un idoneo presupposto giuridico (ad esempio un obbligo di legge) o sia stato lo stesso paziente a chiederlo, previa delega scritta.

Nello sviluppare le piattaforme e le app, perciò, il Garante suggerisce di adottare misure tecniche e organizzative che **impediscano** la diffusione dei dati sulla salute degli utenti che si sono avvalsi dello strumento tecnologico per scegliere il professionista sanitario, in modo da evitare che dei terzi malintenzionati e non autorizzati possano accedere alle informazioni degli utenti; si richiede, in particolare, una peculiare attenzione:

- alle modalità di **accesso** alle app/piattaforme;
- alle modalità di **identificazione** degli utenti in fase di registrazione.

6. LA VALUTAZIONE D'IMPATTO

Prima di mettere online un'app o una piattaforma sanitaria i gestori, quali titolari del trattamento dei dati personali, sono **obbligati** a svolgere una **preventiva valutazione di impatto sul trattamento dei dati**, in virtù del fatto che l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un elevato rischio per i diritti e le libertà delle persone fisiche; i dati sanitari, infatti, se in possesso di chi non è autorizzato a conoscerli possono generare discriminazioni tra i cittadini, che potrebbero vedersi negata, ad esempio, un'assicurazione, un mutuo o un contratto di lavoro sulla base di una malattia.

L'obbligo, in particolare, scaturisce dall'art. 35 del GDPR, perché le app/piattaforme trattano:

- dati sensibili o aventi carattere altamente personale,;
- dati relativi a interessi vulnerabili, tra i quali quelli dei pazienti;
- dati trattati su larga scala (le app/piattaforme sono potenzialmente accessibili a un numero indefinito di utenti nel mondo);
- uso innovativo o applicazione di nuove soluzioni tecnologiche ed organizzative.

I gestori di app/piattaforme sono **obbligati a consultare l'Autorità Garante per la privacy** qualora le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento sui diritti e le libertà degli interessati **non siano ritenute sufficienti**, ovvero quando il **rischio residuale per i diritti e la libertà degli interessati rimanga**, comunque, elevato anche dopo la valutazione d'impatto.

La valutazione d'impatto non deve essere un adempimento da effettuare una tantum, ma deve essere soggetta a continua e costante revisione, anche alla luce dell'evoluzione tecnologica che potrebbe portare a delle falle nei sistemi di sicurezza adottati inizialmente per proteggere i dati degli utenti.

La valutazione di impatto deve contenere:

- la sistematica descrizione dei trattamenti;
- la descrizione delle finalità del trattamento;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i suddetti rischi;
- le garanzie, le misure di sicurezza e i meccanismi necessari per garantire la protezione dei dati personali e dimostrare la conformità al GDPR.

7. RESPONSABILITÀ E RUOLI CONNESSI AL TRATTAMENTO DEI DATI EFFETTUATO TRAMITE PIATTAFORME/APP SANITARIE

In generale, i protagonisti del trattamento dei dati personali sono:

- il titolare
- il contitolare
- il responsabile del trattamento.

Il **titolare del trattamento dei dati personali**, in particolare, è il soggetto che determina le decisioni relative a perché (finalità) e come (modalità) devono essere trattati i dati personali, nel rispetto dei principi generali di:

- **Liceità, correttezza e trasparenza**, in virtù dei quali i dati devono essere trattati in modo legale, corretto e trasparente nei confronti del paziente;

- **limitazione della finalità**, secondo cui i dati devono essere raccolti solo per scopi specifici, legittimi e successivamente trattati in modo coerente con tali scopi;
- **minimizzazione dei dati**, per cui i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto agli scopi del trattamento;
- **esattezza**, che richiede che i dati siano accurati e aggiornati o modificati quando necessario, al verificarsi un loro cambiamento;
- **limitazione della conservazione**, in virtù del quale i dati devono essere conservati solo per un periodo limitato, non oltre quanto necessario per gli scopi del trattamento;
- **integrità e riservatezza**, con garanzia della sicurezza dei dati con misure tecniche e organizzative adeguate a prevenire accessi non autorizzati o perdite;
- **responsabilizzazione**, alla luce del quale il titolare del trattamento deve essere in grado di dimostrare la conformità ai suddetti principi.

Il **responsabile del trattamento dei dati personali**, invece, è il soggetto (persona fisica, giuridica, ente) che elabora i dati personali per conto del titolare del trattamento, in base alle istruzioni da quest'ultimo fornite.

Il titolare e il responsabile del trattamento dei dati personali, nel contesto delle piattaforme e delle app sanitarie, sono identificabili in soggetti differenti, in base alla tipologia di dati trattati; nello specifico, il titolare del trattamento dei dati personali si identifica con il proprietario/gestore della piattaforma per quanto concerne:

1. i dati personali degli utenti, utilizzati per la registrazione e la creazione degli account e per la fornitura dei servizi;
2. i dati personali dei professionisti sanitari, limitatamente a quelli strettamente necessari per l'esecuzione del contratto tra la piattaforma/app e il professionista sanitario.

Il **professionista sanitario** è, invece, **il titolare del trattamento dei dati sulla salute dei pazienti. Il proprietario/gestore della piattaforma**, con riferimento a tali dati, potrebbe solo **eventualmente essere designato quale responsabile del trattamento** da parte del professionista sanitario, ad esempio per la gestione dell'agenda degli appuntamenti, la raccolta,

archiviazione e conservazione della documentazione medica dei pazienti; la designazione deve avvenire attraverso un contratto che preveda, obbligatoriamente, che il responsabile del trattamento:

a. tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b. garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c. adotti tutte le misure richieste ai sensi dell'articolo 32, idonee a garantire l'osservanza dei principi di protezione dei dati personali;
d. rispetti le condizioni di cui ai paragrafi 2 e 4 dell'art. 28 del GDPR per ricorrere a un altro responsabile del trattamento;
e. tenendo conto della natura del trattamento, assista il 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 dell'interessato di cui al capo III;
f. assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 a 36 (sicurezza dei dati personali), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g. su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
h. metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Alla luce di quanto sopra, è scontato che in alcuni casi il titolare del trattamento potrà, **contemporaneamente**, assumere anche il ruolo di responsabile del trattamento dei dati personali: per i dati sanitari, infatti, il professionista medico potrebbe decidere di mantenere per sé il **doppio ruolo**, così come il gestore della piattaforma/app potrebbe inglobare il doppio ruolo per i dati degli utenti o dei professionisti sanitari.

I soggetti proprietari dei dati (pazienti, utenti, medici) devono essere informati in maniera esplicita, chiara e trasparente circa la ripartizione dei ruoli di titolare e responsabile del trattamento dei dati personali, anche ai fini dell'esercizio dei diritti degli interessati, quali:

- informazione e accesso
- rettifica
- cancellazione
- opposizione al processo decisionale automatizzato.

8. LE INFORMAZIONI DA DARE AGLI UTILIZZATORI DELLE PIATTAFORME E DELLE APP SANITARIE

Gli utilizzatori delle piattaforme e delle app sanitarie hanno il diritto ad essere informati dai proprietari circa le modalità di utilizzo, raccolta e conservazione dei loro dati personali nonché circa i ruoli di titolare e responsabile del trattamento dei dati, come sopra definiti, in virtù del principio di trasparenza su cui si fonda il GDPR, e ciò tramite un'apposita informativa facilmente fruibile e comprensibile dagli utenti.

Per quanto concerne **i dati personali degli utenti** che si registrano sulle piattaforme, devono essere illustrati, in particolare:

- i trattamenti svolti dal **proprietario/gestore** della piattaforma in qualità di **titolare** e quelli eventualmente svolti con il ruolo di **responsabile**, evidenziando, per ciascuna di queste fattispecie, le diverse **finalità** del trattamento, le relative **basi giuridiche** e i **tempi di conservazione dei dati**;
- la **natura transfrontaliera o meno del trattamento**, con l'indicazione dell'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare del trattamento o responsabile del trattamento, competente ad agire in qualità di autorità

di controllo capofila, secondo la procedura di cui all'articolo 60 del Regolamento;

- eventuali trattamenti dei dati personali, inclusi quelli sulla salute, per **finalità ulteriori rispetto a quelle di cura**, come ad es. di natura commerciale, avendo cura di indicare per ciascuna finalità la corretta base giuridica del trattamento (quale ad esempio il consenso dell'interessato).

Con particolare attenzione ai dati personali dei professionisti sanitari, invece, il proprietario/gestore della Piattaforma, in qualità di titolare, dovrà fornire ai professionisti sanitari, prima che il trattamento abbia inizio e quindi prima che questi ultimi si registrino alla piattaforma, tutte le informazioni di cui all'art. 13 del Regolamento:

a. l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b. i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d. qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f. ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

Il Garante richiede inoltre ai gestori delle piattaforme/app di porre particolare attenzione, nell'informativa:

- ai criteri in base ai quali viene visualizzato dall'utente l'elenco dei professionisti a seguito della ricerca con particolare riferimento all'eventuale uso di **algoritmi** o sistema di **intelligenza artificiale**;
- a eventuali trattamenti in ordine ai **giudizi di gradimento** espressi dal paziente sul professionista sanitario.

Con riferimento al trattamento dei dati sanitari dei pazienti, la cui titolarità rimane in capo al professionista sanitario, il quale solo eventualmente può nominare quale responsabile il gestore della piattaforma/app, il Garante richiede che:

- prima che il trattamento di cura abbia inizio, sia resa ai propri pazienti **un'autonoma e specifica informativa** con tutti gli elementi di cui all'art. 13 del Regolamento;
- qualora, prima di entrare in contatto con il paziente per l'erogazione delle prestazioni sanitarie, il professionista sanitario decida anche di usufruire dei servizi offerti dalla piattaforma per la gestione del rapporto medico-paziente e ciò comporti un trattamento di dati sulla salute dei propri pazienti da parte della piattaforma per conto del professionista sanitario, in qualità di responsabile, il professionista sanitario può prevedere, nell'atto di designazione ai sensi dell'art. 28 del Regolamento, che l'informativa sia resa al paziente dal proprietario/gestore della piattaforma per conto del predetto professionista;
- qualora la piattaforma sia utilizzata dai professionisti sanitari quali i MMG e dai PLS per gestire le proprie relazioni con i pazienti, i servizi potranno essere offerti solo a seguito di una **espressa richiesta da parte dell'interessato**, il quale dovrà essere **preventivamente e chiaramente informato della facoltatività** di utilizzo di questo canale per entrare in contatto con i suddetti medici.

9. IL TRATTAMENTO TRANSFRONTALIERO

Il trattamento dei dati personali si definisce **transfrontaliero** quando:

a. ha luogo in più di uno Stato membro dell'Unione Europea, in quanto il titolare del trattamento o il responsabile del trattamento sono stabiliti in più di uno Stato membro;
b. il titolare o il responsabile del trattamento operano all'interno di un unico Stato dell'Unione Europea, ma il trattamento dei dati personali incide su soggetti che si trovano in più di uno stato membro.

La problematica dei trasferimenti transfrontalieri dei dati è molto complessa, e ha lo scopo di dare attuazione a due regole fondamentali in materia di tutela dei dati: *one stop shop* (cioè unica Autorità garante) e divieto di *forum shopping* (cioè scelta di collocare la sede in uno Stato piuttosto che in un altro, in base alla malleabilità dell'Autorità Garante).

In pratica, ogni Stato membro dell'Unione ha una sua Autorità Garante in materia di dati personali, e le stesse possono operare in maniera disomogenea tra loro, ispirandosi a criteri diversi sia per la valutazione dei fatti alla base delle violazioni che per la comminazione delle sanzioni.
Lo scopo del GDPR, infatti, è quello di offrire la stessa regolamentazione a tutti i paesi dell'Unione Europea, incentivando la libera circolazione dei dati all'interno dei paesi europei.

Nel caso di trattamento transfrontaliero dei dati, l'Autorità di controllo (cioè il Garante) che ha sede nel luogo in cui si trova lo stabilimento principale o unico in Europa del titolare o del responsabile del trattamento assume il ruolo di Autorità capofila: gli utenti, per esercitare i loro diritti, dovranno perciò rivolgersi a questa Autorità, e dovranno essere informati in maniera adeguata dal titolare e dal responsabile del trattamento, in modo da poter indirizzare eventuali richieste al Garante privacy corretto, anziché "girovagare" tra più Autorità nazionali.

CONSULCESI CLUB

Un servizio di Assicurazione e Consulenti esperti su cui contare

Per scegliere con consapevolezza la soluzione più adatta alle tue esigenze

CONSULCESI CLUB

10. LA SICUREZZA DEL TRATTAMENTO DEI DATI DA PARTE DEI PROPRIETARI E DEI GESTORI DI APP E PIATTAFORME

Il Garante Privacy suggerisce ai proprietari e ai gestori di app e piattaforme dedicate alla sanità di adottare una serie di misure che garantiscano la sicurezza dei dati personali degli utilizzatori, come ad esempio:

a. procedura di adesione alla piattaforma da parte dello specialista che preveda la **verifica del possesso della qualifica professionale** (es. invio di un codice OTP all'indirizzo PEC - censito su INI-PEC - del medesimo professionista);
b. procedura di **verifica/convalida del dato di contatto** scelto dall'utente (es. indirizzo di posta elettronica, numero di cellulare);
c. misure volte alla **riduzione degli errori di omonimia/omocodia**;
d. procedure di **autenticazione informatica a più fattori**;
e. meccanismi di **blocco della app in caso di inattività** (es. time out) o di **chiusura** della medesima;
f. sistemi di **monitoraggio** anche automatici per rilevare **accessi non autorizzati o anomali** alle piattaforme.

In conformità alle Linee Guida Cookie del 2021, eventuali cookies e altri strumenti di tracciamento non strettamente necessari alla fornitura del servizio possono essere utilizzati, purché l'utente abbia espresso il proprio **consenso** e sia stato **adeguatamente informato**.