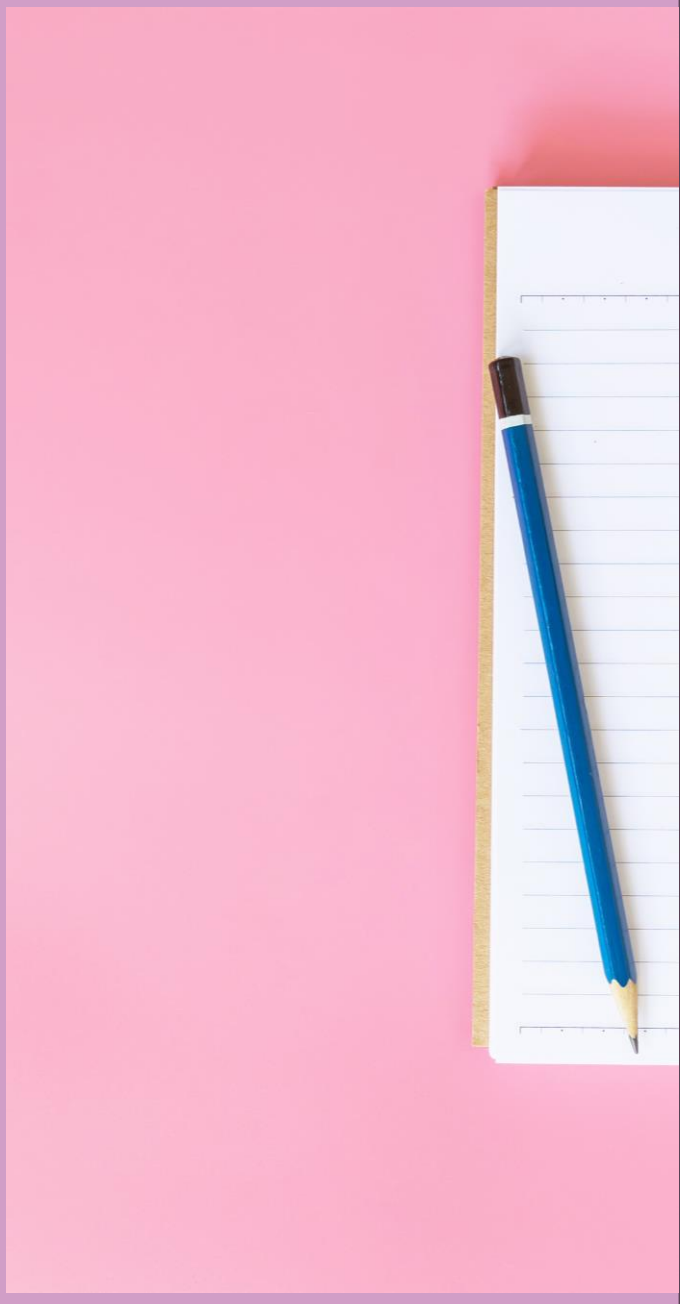
Bird & Bird

Piattaforme per il contatto medico-paziente e trattamento dei dati personali

Le indicazioni del Garante

9 aprile 2024



Piattaforme per il contatto medico-paziente e trattamento dei dati personali

Le indicazioni del Garante

Introduzione

La crescente diffusione delle piattaforme digitali – utilizzabili tramite *web* o *app* – per la prenotazione di visite specialistiche e trattamenti diagnostici sebbene abbia agevolato le attività di contatto nel rapporto medico-paziente, rende necessario al tempo stesso alcune riflessioni per garantire che i dati personali il cui trattamento è insito nell'uso di tali piattaforme avvenga nel rispetto della normativa vigente.

Le soluzioni in questione, infatti, da un lato, facilitano i pazienti nella prenotazione di visite specialistiche e trattamenti diagnostici, potendo selezionare il professionista sanitario in base a specializzazione e zona in cui opera, e agevolano i professionisti nella gestione dei rapporti con i pazienti, della propria agenda e del pagamento delle prestazioni erogate. Dall'altro lato, il ricorso a tali servizi comporta lo scambio di dati personali tra i soggetti coinvolti, a vario titolo e con differenti finalità, nell'utilizzo delle piattaforme stesse (*e.g.,* scambio di documenti sanitari, visualizzazione dello storico degli appuntamenti). In varie occasioni tali dati sono anche idonei a rivelare informazioni sullo stato di salute di chi fruisce dei servizi sottostanti.

In un simile contesto, oltre ai professionisti sanitari e ai pazienti, un ruolo centrale viene svolto anche dai gestori delle soluzioni tecnologiche, che di fatto intervengono nelle attività di trattamento di dati personali al fine di consentire la fruizione dei servizi e si offrono come intermediari nel contatto tra pazienti e professionisti sanitari.

Lo sviluppo e l'utilizzo di tali soluzioni tecnologiche e innovative impone, pertanto, un'attenta valutazione degli aspetti inerenti alla protezione dei dati personali, nel rispetto dei diritti e delle libertà fondamentali degli interessati, soprattutto considerando che il trattamento riguarda anche dati particolarmente sensibili quali quelli relativi allo stato di salute.

Sulla scorta di tali considerazioni, e di alcuni approfondimenti che l'Autorità Garante per la protezione dei dati personali ("**Garante**") aveva condotto nei mesi scorsi, il 28 marzo 2024, il Garante ha pubblicato un documento che riassume in 10 punti gli obblighi e gli adempimenti da rispettare nel contesto del trattamento di dati personali così delicati, il "*Compendio sul trattamento dei dati personali effettuato attraverso piattaforme volte a mettere in contatto i pazienti con i professionisti sanitari accessibili via web e app*" ("**Compendio**").

Il Compendio rappresenta quindi un'utile guida pratica per i gestori delle piattaforme e per i professionisti che se ne avvalgono.

Le indicazioni del Garante

1. Finalità e basi giuridiche del trattamento

Mediante l'utilizzo delle piattaforme in esame, i dati personali degli interessati sono trattati per una pluralità di finalità da diversi attori che intervengono a vario titolo nelle operazioni di trattamento.

In particolare, in questo contesto si possono generalmente distinguere tre macro-tipologie di trattamenti connotate da distinte finalità e basi giuridiche:

a **Trattamento dei dati degli utenti** (anche idonei a rivelare lo stato di salute degli stessi) che utilizzano le piattaforme per la scelta e la prenotazione di una prestazione con un professionista sanitario, e che comporta solitamente la creazione di un proprio *account*. In questo caso, il trattamento è volto a offrire un servizio di carattere amministrativo all'utente dietro sua esplicita richiesta e, pertanto, non può essere ricondotto nel novero dei trattamenti per finalità di cura ai sensi dell'art. 9, par. 2, lett. h) e par. 3 del Regolamento (UE) 2016/679 – **GDPR**. Resta inteso che l'adesione del paziente ai servizi deve restare sempre facoltativa.

   Con riguardo alla base giuridica occorre distinguere in ragione delle tipologie di dati e delle finalità:

   - per il trattamento dei dati sulla salute, non trattandosi di operazioni strettamente necessarie alla diagnosi o terapia sanitaria, è necessario acquisire il preventivo consenso informato degli utenti (art. 9, par. 2, lett. a) del GDPR);
   - per i trattamenti effettuati dalla piattaforma di dati personali degli utenti non appartenenti alle categorie particolari (*e.g.,* informazioni necessarie per la mera creazione dell'*account*) non è necessario acquisire il consenso dell'interessato, in quanto la base giuridica è rappresentata dal rapporto contrattuale sotteso alla registrazione e all'utilizzo della piattaforma (art. 6, par. 1, lett. b) del GDPR);
   - per eventuali trattamenti volti a perseguire ulteriori finalità non compatibili con lo scopo della raccolta dei dati nell'ambito dei servizi offerti delle piattaforme (*e.g.,* invio di comunicazioni commerciali e di *marketing* riguardanti ulteriori servizi offerti dai gestori delle piattaforme), è necessario raccogliere un consenso *ad hoc* per ciascuna finalità ulteriore[1]. Sul punto, il Garante ricorda, inoltre, che sussistono specifiche limitazioni in ordine all'utilizzo dei dati raccolti nell'ambito dei servizi offerti dalle piattaforme per finalità ulteriori (*e.g*., profilazione degli interessati);

b **Trattamento dei dati personali dei professionisti sanitari che si avvalgono delle piattaforme per entrare in contatto con possibili pazienti**. Tale trattamento avviene nel contesto di un rapporto contrattuale tra il gestore della piattaforma e il professionista sanitario e, se del caso, può riguardare altresì la recensione espressa dall'utente sul professionista sanitario. Ne consegue che la base giuridica che legittima il trattamento dei dati dei professionisti sanitari è l'esecuzione del contratto tra le parti (art. 6, par. 1, lett. b) del GDPR).

c **Trattamento di dati sulla salute dei pazienti che potrebbero essere venuti in contatto con il professionista sanitario attraverso la piattaforma – eventualmente effettuati dal professionista, in qualità di titolare del trattamento** – nell'ambito del rapporto medico-paziente (*e.g.,* condivisione di documenti sanitari, come prescrizioni o referti). Tale trattamento è effettuato per finalità di diagnosi e cura da o sotto la responsabilità di un professionista sanitario tenuto al segreto professionale; pertanto, non è necessario il consenso dell'interessato, trovando applicazione l'art. 9, par. 2, lett. h) e par. 3 del GDPR[2].

In aggiunta alle considerazioni relative alle condizioni di liceità applicabili, il Garante pone l'accento sulla necessità di coordinare lo sviluppo delle soluzioni tecnologiche in esame con le disposizioni normative che regolano gli strumenti di sanità digitale con finalità analoghe e/o strettamente connesse a quelle sopra

[1] Cfr. Considerando 32, 42 e 43, artt. 5, 6, par. 1, lett. a) e 7 del GDPR; "*Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679*" adottate il 4 maggio 2020 dal Comitato europeo per la protezione dei dati personali; Sentenza C-673/17, del 1° ottobre 2019 e sentenza C-61/19, dell'11 novembre 2020.
[2] Cfr. "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*" del 7 marzo 2019, doc. *web* 9091942.

descritte[3]. Ciò anche in considerazione del fatto che tali regole rappresentano un utile parametro di riferimento ai fini dell'individuazione, da parte del titolare, delle misure tecniche e organizzative maggiormente idonee a ridurre i rischi del trattamento.

2. Il divieto di diffusione dei dati e l'eventuale comunicazione di dati a terzi

In linea con la normativa in materia di protezione dei dati personali, le informazioni relative allo stato di salute non possono essere oggetto di diffusione. Possono tuttavia essere comunicate a un soggetto diverso dall'interessato esclusivamente in presenza di un idoneo presupposto giuridico, su indicazione dell'interessato stesso o previa delega scritta di quest'ultimo (artt. 2-*septies*, co. 8 e art. 166, co. 2, del D.Lgs. 196/2003 e art. 9 del GDPR).

Nel Compendio è dunque richiamata la necessità che, nello sviluppo delle soluzioni tecnologiche in esame, il titolare del trattamento adotti misure tecniche e organizzative che impediscano la diffusione dei dati sulla salute degli utenti che si sono avvalsi delle piattaforme. In particolare, il Garante pone l'attenzione sui profili inerenti alle modalità di accesso e di registrazione ai servizi, che devono risultare idonee ad escludere il rischio di accesso da parte di soggetti non autorizzati.

Allo stesso modo, misure adeguate volte a evitare la diffusione dei dati trattati mediante le piattaforme devono essere adottate anche dai professionisti sanitari sui quali vige il medesimo divieto di diffusione dei dati relativi alla salute dei pazienti.

3. La valutazione d'impatto

Alla luce della natura dei dati trattati mediante le piattaforme e della potenziale numerosità degli interessati, che potrebbero essere qualificati anche come vulnerabili, il Garante ritiene che il trattamento in esame (*rectius* tutte le citate macro-tipologie di trattamenti descritte) rientri tra quelli che necessitano di una preventiva valutazione d'impatto sulla protezione dei dati ("**DPIA**"), ai sensi dell'art. 35 del GDPR e delle linee guida del Gruppo di Lavoro Articolo 29 (ora *European Data Protection Board*) in merito alla DPIA[4].

Ciò in quanto risultano applicabili ai trattamenti in esame almeno quattro dei criteri definiti dallo *European Data Protection Board* al fine di individuare i casi in cui un trattamento richieda una DPIA. Più precisamente, il Garante fa riferimento ai seguenti criteri: *(i)* "*dati sensibili o aventi carattere altamente personale*"; (ii) "*dati relativi ad interessati vulnerabili*" (ivi inclusi i pazienti); *(iv)* "*trattamento di dati su larga scala*"; e *(iii)* "*uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative*".

Di conseguenza, i trattamenti in questione sono da considerarsi tra quelli "*ad alto rischio*" e richiedono, pertanto, lo svolgimento di una DPIA quale adempimento obbligatorio al fine di individuare le misure idonee a garantire il rispetto dei principi fondamentali del GDPR nonché dei diritti e delle libertà degli interessati.

4. Ruoli privacy, conseguenti adempimenti e responsabilità

Come già evidenziato, nel contesto del trattamento di dati personali per mezzo delle piattaforme in esame sono coinvolti, a vario titolo, una pluralità di soggetti.

Sulla scorta di tale considerazione, il Garante richiama la necessità di definire i ruoli *privacy* di tali soggetti, adottando una visione complessiva delle operazioni di trattamento, che tenga conto delle diverse finalità e dunque delle relative basi giuridiche.

---

[3] Cfr. Disciplina sulla refertazione online di cui al D.P.C.M. 8 agosto 2013; Riforma del Fascicolo Sanitario Elettronico (**FSE**) di cui al D.M. 7 settembre 2023; Decreti del Ministero dell'economia e delle finanze del 25 marzo 2020, del 30 dicembre 2020 e del 15 gennaio 2021.

[4] "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679*" (WP 248 rev.01), come modificate e adottate da ultimo il 4 ottobre 2017 dal Gruppo di Lavoro Articolo 29.

In particolare, partendo dall'esperienza maturata e dai casi già esaminati in relazione alle tre macrocategorie di trattamento illustrate sopra, il Garante individua tre possibili scenari in ordine alla corretta definizione dei ruoli *privacy*:

- Per trattamenti dei dati personali degli utenti: il gestore della piattaforma si qualifica come titolare del trattamento dei dati personali raccolti – nella misura di quanto strettamente necessario – per la registrazione e la creazione degli *account* e per la fornitura di altri servizi messi a disposizione da quest'ultimo;
- Per trattamenti dei dati personali dei professionisti sanitari: il gestore della piattaforma agisce in qualità di titolare del trattamento in relazione ai dati personali dei professionisti sanitari strettamente necessari per l'esecuzione di un contratto di servizi tra le parti;
- Per trattamenti di dati sulla salute dei pazienti – che potrebbero essere venuti in contatto con il professionista sanitario attraverso la piattaforma – eventualmente effettuati dal predetto professionista per finalità di cura: il professionista opera in qualità di titolare del trattamento, mentre, il gestore della piattaforma potrebbe essere designato responsabile del trattamento dal professionista sanitario, qualora effettui trattamenti di tipo tecnico amministrativo per suo conto (*e.g.*, la gestione dell'agenda degli appuntamenti, la raccolta, archiviazione e conservazione della documentazione medica dei pazienti). Resta fermo che, nell'espletamento di tali trattamenti per conto del professionista, il gestore della piattaforma può agire esclusivamente in qualità di responsabile del trattamento e non è autorizzato a trattare i dati sulla salute degli utenti per finalità di cura.

5. Il principio di correttezza e trasparenza e le informazioni da rendere agli interessati

In ossequio al principio di trasparenza, il titolare è tenuto a illustrare all'interessato i dettagli relativi al trattamento in forma chiara e concisa, prima che il trattamento abbia inizio.

Considerando che le piattaforme in questione sono principalmente accessibili tramite un sito *web* e/o un'*app*, e che i trattamenti effettuati mediante le stesse perseguono molteplici finalità, il Garante raccomanda l'uso di informative stratificate o progressive, consentendo così all'utente di consultare le specifiche sezioni di interesse.

Tenendo sempre conto delle tre macro-tipologie di trattamento sopra richiamate, il Garante sottolinea l'importanza di fornire tutte le informazioni di cui agli art. 13 e 14 del GDPR, con particolare attenzione alle seguenti informazioni:

a. trattamenti dei dati personali degli utenti che si registrano sulle piattaforme: *(i)* i trattamenti svolti dal gestore della piattaforma in qualità di titolare e quelli eventualmente svolti con il ruolo di responsabile, evidenziando per ciascuna le finalità e le basi giuridiche del trattamento, nonché i tempi di conservazione dei dati; *(ii)* eventuali trattamenti dei dati personali, inclusi quelli sulla salute, per finalità ulteriori rispetto a quelle di cura. Inoltre, in aggiunta alle informazioni richieste dall'art. 13 del GDPR, il Garante precisa la necessità di specificare la natura transfrontaliera o meno del trattamento con l'indicazione dell'autorità di controllo competente ad agire in qualità di autorità di controllo capofila;

b. trattamenti dei dati personali dei professionisti sanitari: il gestore della piattaforma deve specificare con cura al professionista sanitario: *(i)* i criteri in base ai quali l'utente visualizza l'elenco dei professionisti a seguito della ricerca, con particolare riferimento all'eventuale uso di algoritmi o sistema di intelligenza artificiale e *(ii)* eventuali trattamenti in ordine ai giudizi di gradimento espressi dal paziente sul professionista sanitario;

c. trattamenti di dati sulla salute dei pazienti – che potrebbero essere venuti in contatto con il professionista sanitario attraverso la piattaforma – eventualmente effettuati dal professionista per finalità di cura, in qualità di titolare. Con riferimento a tale scenario, il Garante ricorda che:

   - prima che il trattamento di cura abbia inizio, il professionista sanitario deve rendere ai propri pazienti un'autonoma e specifica informativa conforme all'art. 13 del GDPR;
   - 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 in qualità di responsabile, nell'atto di designazione è possibile stabilire che l'informativa sia resa al paziente dal gestore della piattaforma per conto del predetto professionista;

- qualora la piattaforma sia utilizzata dai professionisti sanitari 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 tale canale per entrare in contatto con i medici.

6. Trattamenti effettuati al di fuori del territorio nazionale

A seguito di varie istruttorie effettuate dal Garante è emerso che spesso le piattaforme sono gestite da soggetti stabiliti fuori dall'Italia, pertanto, il trattamento sotteso all'utilizzo di tali strumenti può assumere la natura di trattamento transfrontaliero.

In tal caso, come previsto dall'art. 56 del GDPR, l'autorità di controllo che ha sede nel luogo in cui si trova lo stabilimento principale o unico nell'UE del titolare o responsabile del trattamento, assume il ruolo di autorità capofila, alla quale viene trasferita la competenza da tutte le altre autorità di controllo interessate.

Sul punto, il Garante specifica la necessità di portare a conoscenza degli interessati la natura transfrontaliera del trattamento prima che il trattamento abbia inizio, al fine di informarli che, l'eventuale presentazione di un reclamo all'autorità interessata determinerà l'avvio della c.d. procedura di cooperazione tra l'autorità capofila e le diverse autorità interessate ai sensi dell'art. 60 del GDPR.

Laddove il trattamento coinvolga altresì soggetti stabiliti presso paesi al di fuori dello Spazio Economico Europeo, si applicano le disposizioni di cui agli artt. 45 e ss. del GDPR, fermo restando la necessità di informare l'interessato di tali operazioni, in particolare, con riguardo al presupposto legittimante il trasferimento e le garanzie adeguate che si intendono prevedere.

7. Il principio di privacy by design e le misure di sicurezza

In virtù dei principi di *privacy by design* e *privacy by default*, il titolare del trattamento è tenuto ad adottare, sin dalla fase di disegno e progettazione del trattamento, misure di sicurezza tecniche e organizzative adeguate, nonché a valutarne costantemente l'idoneità rispetto ai rischi e vulnerabilità sottesi al trattamento.

Nell'ipotesi in esame, anche in considerazione della natura dei dati trattati, in ossequio all'art. 25 del GDPR, il titolare deve aver cura di individuare misure tecniche e organizzative volte a ridurre il rischio di distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati.

Tra le misure che i gestori delle piattaforme devono prevedere, a titolo esemplificativo e non esaustivo, il Garante menziona le seguenti:

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

Conclusioni

«*La rapidità dell'evoluzione tecnologica e la globalizzazione comportano sempre nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali*» (considerando 6, GDPR).

Il monito del legislatore europeo cristallizzato nel considerando 6 del GDPR (a circa otto anni di distanza) è attuale e veritiero ancora oggi. La disciplina della protezione dei dati personali deve necessariamente stare al passo dell'evoluzione tecnologica e della digitalizzazione dei servizi: le persone fisiche devono avere il controllo dei dati personali che le riguardano, soprattutto nei contesti digitali, potendo contare su una certezza giuridica e operativa rafforzata.

Regole certe, linee guida e documenti di indirizzo giocano, dunque, un ruolo fondamentale per creare quell'imprescindibile clima di consapevolezza e fiducia (tanto per gli individui, quanto per le imprese) che è in grado di garantire un corretto e coerente sviluppo dell'economia digitale nel mercato interno dell'Unione.

In un simile scenario, il Compendio rappresenta pertanto un'utile guida di taglio pratico per gli operatori coinvolti nello sviluppo, erogazione e utilizzo delle piatteforme per la gestione dei rapporti tra medico e paziente. Le indicazioni ivi contenute chiariscono, o confermano, numerosi aspetti la cui corretta definizione risulta essenziale al fine di disegnare i trattamenti di dati personali sottesi all'utilizzo di applicazioni e portali dedicati in conformità alla normativa applicabile.

L'auspicio è, dunque, che il Compendio contribuisca da un lato a supportare ulteriormente il livello di sicurezza e *compliance* delle soluzioni tecnologiche disponibili sul mercato (o di futuro sviluppo) e, dall'altro lato, ad accrescere la fiducia degli utenti/pazienti in simili strumenti di semplificazione e digitalizzazione degli adempimenti connessi alle prestazioni sanitarie.

Concludendo, il Compendio potrebbe, al tempo stesso, rappresentare uno strumento di riflessione e guida con riferimento all'implementazione di altri servizi e soluzioni tecnologiche che il mercato sta già iniziando a fornire agli operatori sanitari e ai pazienti, come ad esempio applicazioni di supporto ai pazienti per ottenere informazioni, gestire promemoria e ricevere notifiche sui farmaci in uso, oppure piattaforme e applicazioni per la gestione dei *Patient Support Program*[5] che prevedano la partecipazione di più stakeholders (*e.g.*, professionisti sanitari, azienda farmaceutica, fornitore della soluzione tecnologica, pazienti, *caregiver*, *etc*.).

[5] «*Si definisce Patient Support Program (PSP) una iniziativa che ha per finalità la messa a disposizione da parte dell'azienda farmaceutica di servizi addizionali e non sostituivi a quelli in capo all'Ente o al SSN a diretto beneficio del paziente in trattamento con uno specifico farmaco già autorizzato all'immissione in commercio.*» (art. 4.7, Codice Deontologico Farmindustria).

Contatti

Adriano D'Ottavio

Counsel

+390669667000
adriano.dottavio@twobirds.com

Debora Stella

Counsel

+390230356000
debora.stella@twobirds.com

Lavinia Nappi

Associate

+390669667000
lavinia.nappi@twobirds.com

Sveva Placidi

Trainee

+390669667000
sveva.placidi@twobirds.com

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Shenzhen • Singapore • Stockholm • Sydney • Warsaw