GPDP

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

MARZO 2024

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

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

MARZO 2024

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Premessa

Il presente compendio intende fornire delle preliminari indicazioni sul trattamento dei dati personali anche relativi alla salute effettuato attraverso piattaforme -utilizzabili tramite *web* e/o *App*- volte a facilitare la messa in contatto degli utenti con i professionisti sanitari, ivi compresi i Medici di medicina generale (MMG) e i pediatri di libera scelta (PLS).

In particolare, tali strumenti digitali offrono servizi di prenotazione di visite specialistiche e trattamenti diagnostici, consentendo all'utente di scegliere il professionista in base alla specializzazione e alla zona in cui opera e al professionista sanitario di gestire in modo più semplice (grazie alla tecnologia offerta) i rapporti con i propri pazienti, la propria agenda (prenotazione, cancellazione e spostamento degli appuntamenti), le televisite, laddove il servizio è offerto, nonché il pagamento delle prestazioni erogate.

Tali strumenti, in alcuni casi, consentono di inviare e archiviare documenti sanitari, anche al fine di condividerli con il professionista sanitario prima di un appuntamento o durante il rapporto di cura instaurato con lo stesso e ulteriori servizi a beneficio degli utenti, quale quello di visualizzazione dello storico degli appuntamenti e di ricevere via *email* informazioni sulla salute pubblica e comunicazioni promozionali sui servizi offerti.

Resta fermo che i proprietari e gestori delle piattaforme in esame non sono legittimati a trattare i dati sulla salute degli utenti per finalità di diagnosi, assistenza e terapia sanitaria, che sono invece perseguibili esclusivamente da un professionista sanitario soggetto al segreto professionale, conformemente al diritto unionale e nazionale (art. 9, par. 2 lett. h) e par. 3 del Regolamento). Pertanto, i proprietari e gestori delle piattaforme potranno effettuare solo i trattamenti strettamente necessari ad offrire servizi funzionali al rapporto medico paziente, quali quelli di natura amministrativa (es. pagamento delle prestazioni sanitarie) o tecnologica (es. gestione degli account e degli appuntamenti delle visite specialistiche).

Da ciò emerge che attraverso le predette piattaforme, che nella maggior parte dei casi fanno capo a Società stabilite in paesi europei diversi dall'Italia o in Paesi terzi, i dati personali degli interessati sono trattati per molteplici finalità da diversi soggetti che intervengono a vario titolo nelle operazioni di trattamento. E' dunque essenziale che i profili di protezione dei dati personali siano correttamente indirizzati in omaggio al principio di responsabilizzazione

in base al quale il titolare del trattamento deve conformarsi ed essere in grado di comprovare sia il rispetto dei principi e degli adempienti previsti dal Regolamento e sia di avere effettivamente tutelato il diritto alla protezione dei dati personali degli interessati fin dalla progettazione e per impostazione predefinita (artt. 5, par. 2, 24 e 25 par. 1 del Regolamento).

Pertanto, il presente compendio intende individuare i principali aspetti di protezione dei dati che i titolari devono osservare nella realizzazione dei servizi digitali volti a mettere in contatto i pazienti con i professionisti sanitari, richiamando solo i principali adempimenti relativi ad eventuali attività sanitarie effettuate dai predetti professionisti attraverso l'utilizzo delle suddette piattaforme (es. televisita) con riferimento alle quali è necessario che questi ultimi, in qualità di titolari e in ossequio ai principi di *accountability* e di protezione dei dati fin dalla progettazione*,* conformino i trattamenti alla disciplina in materia di protezione dei dati personali.

Eventuali trattamenti di dati personali posti in essere dal professionista sanitario che è entrato in contatto con il paziente attraverso tali piattaforme, ivi compresi i possibili ulteriori usi delle stesse per inviare e visualizzare documenti con il paziente, devono infatti essere considerati in modo distinto e dovranno essere effettuati da o sotto la responsabilità di ciascun professionista vincolato al segreto professionale, in quanto finalizzati alla diagnosi o alla terapia sanitaria.

Ulteriori trattamenti che possono essere effettuati dal proprietario/gestore della piattaforma richiedono, in omaggio al principio di *accountability,* di essere puntualmente valutati sotto il profilo della finalità del trattamento e della relativa condizione di liceità (art. 5, par. 1, lett. a) e b) del Regolamento).

1. Le finalità del trattamento

In via preliminare, si rappresenta che, ai sensi del Regolamento, si considerano "*dati relativi alla salute*" i 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 (art. 4, par. 1, n. 15, del Regolamento). Il considerando n. 35 del Regolamento precisa poi che i dati relativi alla salute "*comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria"; "un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari*".

Con specifico riferimento alle particolari categorie di dati, tra cui rientrano i dati sulla salute, l'art. 9 del Regolamento sancisce un generale divieto al trattamento a meno che non ricorra una delle specifiche esenzioni a tale divieto, tra le quali sono previsti il consenso dell'interessato e i trattamenti strettamente necessari per finalità di cura svolti da professionisti sanitari soggetti al segreto professionale (artt. 9, par. 2, lett. a) e h) del Regolamento; cfr. provv.to di "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*", del 7 marzo 2019, doc. *web* n. 9091942).

I trattamenti di dati personali effettuati attraverso tali piattaforme, presi in considerazione nel presente compendio, sono finalizzati principalmente ad agevolare l'utente nella scelta del professionista sanitario cui rivolgersi e a facilitare la comunicazione con lo stesso. Si tratta pertanto di un servizio di carattere amministrativo correlato ad una futura ed eventuale prestazione sanitaria.

Ciò stante, si evidenzia che attraverso le suddette piattaforme possono essere effettuate tre macro tipologie di trattamenti caratterizzati da distinte finalità e basi giuridiche:

1. trattamento dei dati degli utenti, che potrebbero essere anche idonei a rivelare lo stato di salute degli stessi (es. in relazione alla tipologia di prestazione sanitaria richiesta o alla specializzazione del professionista sanitario), che utilizzano le predette piattaforme per scegliere e prenotare una prestazione con un professionista sanitario (es. creazione dell'*account)*. Tale trattamento è volto a offrire un servizio di carattere amministrativo all'utente dietro sua esplicita richiesta e pertanto non può essere ricondotto ai trattamenti per finalità di cura di cui all'art. 9, par. 2, lett. h) e par. 3 del Regolamento, che possono essere effettuati esclusivamente da un professionista sanitario soggetto al segreto professionale;
2. trattamento dei dati personali dei professionisti sanitari che si avvalgono delle piattaforme per entrare in contatto con possibili pazienti. Tale trattamento è effettuato nell'ambito di un rapporto contrattuale tra il soggetto proprietario/gestore della piattaforma e il professionista sanitario e può riguardare anche la recensione eventualmente espressa dall'utente sul professionista sanitario;
3. 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, in

qualità di titolare del trattamento- nell'ambito del rapporto medico – paziente (es. condivisione di documenti sanitari, come prescrizioni o referti). Tale trattamento è effettuato per finalità diagnosi e cura da o sotto la responsabilità di un professionista sanitario tenuto al segreto professionale (art. 9 par. 2, lett. h) e par. 3 del Regolamento).

L'adesione a tali servizi da parte dell'utente, non essendo prevista da nessuna disposizione normativa, deve intendersi come facoltativa anche qualora tali strumenti siano offerti da professionisti sanitari convenzionati con il Servizio Sanitario Nazionale come il MMG o il PLS.

2. Il coordinamento con la disciplina vigente sui principali strumenti di sanità digitale

La realizzazione delle predette piattaforme deve necessariamente tener conto delle disposizioni normative che regolano gli strumenti di sanità digitale che hanno finalità analoghe e/o strettamente connesse a quelle sopra descritte.

Per i profili legati alla protezione dei dati personali, si richiama in particolare, la disciplina sulla refertazione *on-line* di cui al d.p.c.m. dell'8 agosto 2013, su cui l'Autorità ha espresso il proprio parere il 6 dicembre del 2012 (doc. *web* n. 2223206), che prevede regole e misure per la consegna di referti al paziente con modalità digitali.

Come recentemente ricordato dal Garante, il legislatore ha poi espressamente disciplinato gli strumenti mediante i quali i professionisti sanitari possono consultare referti e documentazione sanitaria afferente al paziente che hanno in cura, come il Fascicolo sanitario elettronico (FSE), con riferimento al quale sono state individuate misure omogenee sul territorio nazionale a tutela delle libertà e dei diritti fondamentali dell'interessato e dei parametri di qualità e integrità dei dati personali trattati (cfr. parere del 22 agosto 2022 e dell'8 giugno 2023 doc. *web* nn. 9802729 e 9900433). In particolare, la recente riforma del FSE, su cui il Garante ha espresso il richiamato parere l'8 giugno 2023, prevede che sia proprio il MMG/PLS a compilare una partizione del Fascicolo denominata "Profilo sanitario sintetico", nonché a poter accedere a tutti i documenti sanitari presenti nel FSE (*decreto del Ministero della salute, del 7 settembre 2023 - in G.U. n. 249 del 24 ottobre 2023*).

Si richiamano infine i recenti interventi normativi in tema di prescrizione elettronica volti a disciplinare in modo unitario la generazione e la consegna

delle prescrizioni digitali ai pazienti anche da parte dei MMG/PLS (decreti del Ministero dell'economia e delle finanze del 25 marzo 2020, del 30 dicembre 2020 e del 15 gennaio 2021).

Appare necessario inoltre richiamare la differenza, più volte evidenziata dall'Autorità, tra le piattaforme oggetto del presente compendio e gli strumenti di telemedicina, intesa, quest'ultima, come l'insieme delle tecniche mediche ed informatiche che permettono la cura di un paziente da remoto (es. televisita, telemonitoraggio). Tale differenza si fonda proprio sulle diverse finalità perseguite da tali strumenti: finalità di cura per la telemedicina, offerta di un servizio tecnologico nel caso delle predette piattaforme (cfr. FAQ doc. *web* n. 9328079).

Si evidenzia pertanto la necessità che le piattaforme in esame siano sviluppate in modo tale da rispettare i limiti e gli ambiti di applicazione normativamente previsti per gli strumenti di sanità digitale disciplinati dal nostro ordinamento, con particolare riguardo ai limiti e ai vincoli normativi previsti per la refertazione *on-line* e per le prescrizioni elettroniche.

Tali disposizioni rappresentano peraltro un parametro di riferimento per il titolare che intenda sviluppare le predette piattaforme anche ai fini dell'individuazione delle misure tecniche e organizzative più idonee a ridurre gli specifici rischi del trattamento.

3. Le basi giuridiche dei diversi trattamenti svolti dalle società che forniscono i richiamati servizi e dai professionisti sanitari

Come evidenziato nel primo punto del presente compendio, attraverso le suddette piattaforme possono essere effettuati tre macro tipologie di trattamenti, caratterizzati da distinte finalità, con riferimento alle quali rilevano specifiche basi giuridiche.

1. Per il trattamento dei dati sulla salute degli utenti che utilizzano le piattaforme per scegliere e prenotare una prestazione con un professionista sanitario, non trattandosi di operazioni strettamente necessarie alla diagnosi o terapia sanitaria, il titolare del trattamento è tenuto ad acquisire il preventivo consenso informato degli utenti (art. 9, par. 2., lett. a) del Regolamento). Tale manifestazione di volontà deve essere espressa attraverso un atto positivo con il quale l'interessato manifesta una volontà libera, specifica, informata e inequivocabile e revocabile relativa al trattamento dei dati personali

che lo riguardano. Per i trattamenti effettuati dalla piattaforma di dati personali degli utenti non appartenenti alle categorie particolari (es. mera creazione dell'*account*) non sarà necessario acquisire il consenso dell'interessato ai sensi dell'art. 6, par. 1, lett. b) del Regolamento.

Qualora il trattamento sia volto a perseguire ulteriori finalità non compatibili con lo scopo della raccolta (quali ad esempio, quelle relative all'invio di comunicazioni commerciali e di *marketing* riguardanti ulteriori servizi offerti dai soggetti proprietari/gestori delle piattaforme), il consenso dovrà essere prestato per ciascuna di tali finalità (Considerando 32, 42 e 43, artt. 5, 6, par. 1, lett. a) e 7 del Regolamento e Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679, adottate dal Comitato europeo per la protezione dei dati personali, il 4 maggio 2020; sent. C-673/17, del 1° ottobre 2019 e C-61/19, dell'11 novembre 2020).

Si evidenzia inoltre che sussistono specifiche limitazioni in ordine all'utilizzo dei dati raccolti nell'ambito dei servizi offerti dalle piattaforme per finalità ulteriori rispetto a quelle della raccolta e non compatibili con le stesse (profilazione degli interessati sulla base dei cd "real world data", cfr. il provv. del 1° giugno 2023, doc. *web* 9913795).

2. Per il trattamento dei dati personali dei professionisti sanitari che si avvalgono delle piattaforme per entrare in contatto con possibili pazienti, si rappresenta che lo stesso è lecito nella misura in cui è necessario per l'esecuzione di un contratto di servizi tra il soggetto che gestisce la piattaforma e lo stesso professionista sanitario (art. 6, par. 1, lett. b) del Regolamento).
3. Per i trattamenti di dati sulla salute dei pazienti -che potrebbero essere venuti in contatto con il professionista sanitario attraverso la piattaforma- strettamente necessari per le finalità di cura, eventualmente effettuati dal professionista tenuto al segreto professionale, in qualità di titolare del trattamento, nell'ambito del rapporto medico – paziente, fermi restando i limiti normativi indicati nel precedente punto 2) del presente compendio, non sarà necessario acquisire il consenso dell'interessato applicandosi la fattispecie di cui all'art. 9, par. 2, lett. h) e par. 3 del Regolamento (cfr. provvedimento di "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*" del 7 marzo 2019, cit.).

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

La disciplina in materia di protezione dei dati personali prevede che le informazioni sullo stato di salute non possano essere diffuse e possano essere comunicate a un soggetto diverso dall'interessato esclusivamente sulla base di un idoneo presupposto giuridico o su indicazione dell'interessato stesso o previa delega scritta di quest'ultimo (artt. 2-*septies*, comma 8 e art. 166, comma 2, del Codice e art. 9 Regolamento).

Ciò stante, il titolare del trattamento deve quindi prevedere, nello sviluppare le predette piattaforme, l'adozione di misure tecniche e organizzative che impediscano la diffusione dei dati sulla salute degli utenti che si sono avvalsi delle stesse piattaforme per la scelta del professionista sanitario a cui rivolgersi per motivi di salute. Il divieto, ovviamente, opera anche con riferimento agli eventuali trattamenti di dati sulla salute effettuati attraverso la piattaforma dal professionista sanitario in qualità di titolare del trattamento.

Al riguardo, si richiama l'attenzione sulle modalità di accesso alle piattaforme con particolare riferimento a quelle individuate per identificare gli utenti in fase di registrazione che devono risultare idonee a scongiurare il rischio che soggetti non autorizzati possano accedere alle informazioni inserite dagli utenti per la scelta del professionista sanitario, in assenza di un idoneo presupposto giuridico.

5. La valutazione d'impatto

Il Regolamento introduce l'obbligo per i titolari di svolgere una preventiva valutazione di impatto sul trattamento che "*prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 35), e di consultare l´Autorità di controllo 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 le libertà degli interessati resti elevato (art. 36).

A tale riguardo, si segnalano le *Linee guida* concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "*possa presentare un rischio elevato*"[1]. In tale ambito il Gruppo articolo 29 indica

[1] WP248rev.01, adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017.

- la necessità di considerare la valutazione d'impatto non come un adempimento statico da effettuare *una tantum* ma come un processo soggetto a revisione continua.

La valutazione d'impatto deve contenere, oltre ad una descrizione sistematica dei trattamenti e delle finalità del trattamento, una valutazione dei rischi per i diritti e le libertà degli interessati e delle misure conseguentemente previste per affrontare tali rischi, includendo le garanzie, le misure di sicurezza e i necessari meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento (Linee-guida *cit*.).

Le misure individuate dal titolare devono essere volte all'effettiva applicazione dei principi di protezione dei dati personali ponendo i titolari del trattamento nella condizione di comprovare l'idoneità delle stesse, tenuto anche conto degli specifici rischi connessi al trattamento effettuato.

Ciò stante, tenuto conto della natura dei dati trattati attraverso le citate piattaforme e della potenziale numerosità dei soggetti interessati, che potrebbero essere qualificati anche come vulnerabili, il trattamento in esame rientra senza dubbio nei casi in cui il titolare non può prescindere da una preventiva valutazione d'impatto sulla protezione dei dati, ai sensi dell'art. 35 del Regolamento e dei criteri individuati nelle citate Linee guida.

Nella fattispecie in esame infatti ricorrono certamente almeno quattro dei criteri indicati dal Comitato Europeo per la protezione dei dati per individuare i casi in cui un trattamento debba formare oggetto di una valutazione di impatto ai sensi dell'art. 35 del Regolamento. In particolare, si fa riferimento ai seguenti criteri: "*dati sensibili o aventi carattere altamente personale*", "*dati relativi ad interessati vulnerabili*" tra i quali si annoverano i pazienti; "*trattamento di dati su larga scala*", e "*uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative*" (cfr. Linee guida cit., punti 4), 5) e 8; e provv. del 12 marzo 2020, doc. *web* n. 9310804, provv. del 13 maggio 2021, doc. *web* n. 9687977).

Tali trattamenti rientrano dunque, tra quelli ad "*alto rischio*" per i quali la preventiva valutazione d'impatto si rende necessaria in quanto strumento fondamentale per l'individuazione delle misure idonee a tutelare i diritti e le libertà fondamentali degli interessati e a garantire il rispetto dei principi generali del Regolamento, nonché per consentire l'analisi della proporzionalità dei trattamenti effettuati.

Pertanto, alla luce dei suddetti elementi, la valutazione d'impatto si ritiene un adempimento obbligatorio per tutte le citate macro-tipologie di trattamenti effettuati attraverso le piattaforme.

L'assenza di tale valutazione d'impatto non consentirebbe di effettuare, a cura di ciascun titolare del trattamento, un esame complessivo e preventivo sull'adeguatezza e sulla proporzionalità delle misure che si intendono implementare. Ciò, a maggior ragione tenuto conto che attraverso le piattaforme si effettuano trattamenti di dati sulla salute anche da parte di professionisti convenzionati con il sistema sanitario nazionale (MMG e PLS), per i quali si rende pertanto necessario che vengano predisposte misure tecniche e organizzative atte ad assicurare un'effettiva tutela dei diritti e delle libertà fondamentali degli interessati nel pieno rispetto della disciplina di settore agli stessi applicabile in parte sopra richiamata (cfr. punto 2 del presente compendio).

6. Ruoli privacy, conseguenti adempimenti e responsabilità

Nell'ambito delle operazioni di trattamento in esame diversi sono i soggetti a vario titolo coinvolti, rispetto ai quali occorre individuare correttamente i ruoli di titolare (artt. 4, n. 7 e 24) e, se del caso, di contitolare e di responsabile (artt. 4, n. 8 e 28 del Regolamento).

Il titolare è il soggetto che, alla luce del concreto contesto nel quale avviene il trattamento, determina le decisioni di fondo relative a finalità e modalità di un trattamento effettuato in base a uno dei presupposti di liceità di cui agli artt. 6 e 9 del Regolamento (*cfr.* Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR - Versione 2.0 - adottate il 7 luglio 2021 dal Comitato Europeo per la protezione dei dati[2]).

La figura del responsabile rimane invece connotata dallo svolgimento di operazioni di trattamento di dati personali delegate dal titolare il quale, all'esito di proprie scelte organizzative, può individuare un soggetto particolarmente qualificato allo svolgimento delle stesse in termini di conoscenze specialistiche, di affidabilità e di risorse per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento (cfr. il considerando 81 del Regolamento), delimitando l'ambito delle rispettive attribuzioni e fornendo specifiche istruzioni sui trattamenti da effettuare (cfr. Linee guida cit.).

In relazione al ruolo di responsabile del trattamento, è necessario che il titolare designi il soggetto esterno, preposto allo svolgimento di determinate

[2] Disponibili in: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_it

attività che comportano il trattamento di dati personali, come "*responsabile del trattamento*" ai sensi dell'art. 28 del Regolamento.

In caso contrario, in mancanza di tale designazione, la messa a disposizione di dati personali a soggetti esterni si configura come una comunicazione di dati personali da effettuarsi conformemente al quadro normativo vigente e sulla base di un idoneo presupposto giuridico (artt. 5, 6 e 9 del Regolamento).

In ogni caso, le persone fisiche che, anche presso il soggetto esterno, materialmente trattano i dati personali devono essere autorizzate al trattamento e opportunamente istruite ai sensi degli artt. 29 del Regolamento e 2-*quaterdecies* del Codice.

Con specifico riferimento ai trattamenti in esame, fermo restando che la definizione dei ruoli può essere regolata con diverse modalità, in un'ottica di *governance* dei dati è necessario individuare tali ruoli avendo una visione complessiva delle operazioni di trattamento che tenga conto delle diverse finalità per le quali i trattamenti sono svolti e dunque delle diverse basi giuridiche sulle quali essi si fondono.

In particolare, la qualità di titolare non può essere scissa in un livello concreto e in uno formale in quanto essa implica sempre il potere di prendere tutte le decisioni in ordine alle finalità e alle modalità di trattamento compreso il potere di delegare le attività esecutive del trattamento ad altro soggetto. Più precisamente, il fatto che vengano delegate specifiche attività ad un altro soggetto non fa venir meno la qualifica di titolare che anzi costituisce un presupposto per la preposizione del responsabile del trattamento ai sensi dell'art. 28 del Regolamento. Di conseguenza, il titolare, in quanto tale, rimane altresì soggetto all'esercizio dei diritti degli interessati di cui agli artt. da 15 a 22 del Regolamento (cfr. Cass. n. 6927 del 26 febbraio 2016).

Alla luce dell'esperienza maturata, anche in relazione ai casi già esaminati dall'Autorità, rispetto alle tre macro tipologie di trattamento sopra individuate, si illustrano tre possibili scenari in ordine all'individuazione dei ruoli del trattamento:

1. <u>Per trattamenti dei dati personali degli utenti</u>: il proprietario/gestore della Piattaforma assume il ruolo di titolare del trattamento dei dati strettamente necessari che siano raccolti per la registrazione e la creazione degli *account* e per la fornitura di altri servizi messi a disposizione da quest'ultimo (es. visualizzazione dello storico degli appuntamenti, invio di comunicazioni per ricevere informazioni sulla salute pubblica e comunicazioni promozionali sui servizi offerti);

2. Per trattamenti dei dati personali dei professionisti sanitari: il proprietario/gestore della Piattaforma assume il ruolo di titolare del trattamento dei dati personali dei professionisti sanitari strettamente necessari per l'esecuzione di un contratto di servizi tra le parti;
3. Per trattamenti di dati sulla salute dei pazienti -che potrebbero essere venuti in contatto con il professionista sanitario attraverso la piattaforma, in occasione, ad esempio della prenotazione di una visita specialistica, - eventualmente effettuati dal predetto professionista per finalità di cura, lo stesso professionista opera in qualità di titolare del trattamento ed è pertanto tenuto a trattare i dati nel rispetto della specifica disciplina sul trattamento dei dati personali per tali finalità - nell'ambito del rapporto medico – paziente (art.9, par. 2, lett. h) e par. 3 del Regolamento e artt. 75 e ss. del Codice). Rispetto a tali trattamenti il proprietario/gestore della piattaforma potrebbe essere designato responsabile del trattamento dal professionista sanitario, qualora effettui trattamenti di tipo tecnico amministrativo per suo conto quale, ad esempio, la gestione dell'agenda degli appuntamenti, la raccolta, l'archiviazione e la conservazione della documentazione medica dei propri pazienti. Resta fermo, che nell'espletamento di tali trattamenti, per conto del professionista (titolare del trattamento), il proprietario/gestore della piattaforma può agire esclusivamente in qualità di responsabile del trattamento; in tale specifico ruolo, quindi, esso non è autorizzato a trattare i dati sulla salute degli utenti per finalità di cura.

   In tal caso, l'atto di designazione (il contratto o altro atto giuridico) dovrà recare tutti gli elementi di cui all'art. 28, par. 3 del Regolamento, in particolare, le istruzioni sul trattamento dei dati, l'indicazione di tutte le misure di sicurezza tecniche ed organizzative richieste ai sensi dell'articolo 32, che il predetto responsabile è tenuto ad implementare.

Resta quindi fermo che in relazione ai trattamenti in esame possono verificarsi situazioni in cui uno stesso soggetto (ad esempio il gestore della piattaforma) può assumere sia il ruolo di titolare per taluni trattamenti che di responsabile per altri trattamenti.

In ragione di ciò, è fondamentale che, una volta definiti i ruoli di protezione dati dei diversi soggetti, essi siano correttamente rappresentati agli interessati, in quanto ciò si riflette non solo nella individuazione delle corrette basi giuridiche del trattamento e sull'imputazione delle rispettive responsabilità, ma anche sugli obblighi di trasparenza che sono alla base della autodeterminazione informativa

degli interessati, ciò anche ai fini dell'esercizio dei diritti che il Regolamento riconosce agli interessati (artt. da 15 a 22 del Regolamento).

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

I principi di trasparenza e correttezza implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità e che i dati personali siano trattati fornendo preventivamente agli interessati le informazioni di cui all'art. 13 del Regolamento, in caso di dati raccolti direttamente presso di essi, ovvero ai sensi dell'art. 14, in caso di dati raccolti presso soggetti terzi. Tale principio impone che le informazioni e le comunicazioni relative al trattamento dei dati personali siano rese in una forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (cons. 39, 58 e art. 12 del Regolamento).

L'obbligo di fornire agli interessati le informazioni in forma "*concisa e trasparente*" implica che il titolare del trattamento presenti le informazioni in maniera efficace e succinta al fine di evitare una sovraesposizione informativa. Esse dovrebbero essere "*concrete e certe, non dovrebbero essere formulate in termini astratti o ambigui né lasciare spazio a interpretazioni multiple*" (cfr. punti 8 e 12, delle Linee guida sulla trasparenza ai sensi del regolamento 2016/679, adottate dal Gruppo Articolo 29, il 29 novembre 2017, versione emendata adottata l'11 aprile 2018 e paragrafo e paragrafo 3.7).

In ossequio al principio di trasparenza devono quindi risultare chiare, prima che il trattamento abbia inizio, in particolare sia le finalità perseguite, che le distinte e corrispondenti basi giuridiche del trattamento.

La disponibilità di queste informazioni è infatti fondamentale per ottenere il consenso al trattamento dei dati personali dell'utente, laddove necessario, che può ritenersi valido solo se l'interessato è stato previamente informato in merito agli elementi chiave del trattamento dei dati e quindi consapevole delle scelte in materia di trattamento dei dati che sta effettuando attraverso la manifestazione del consenso. Inoltre, si dovrebbe comunicare agli utenti con un linguaggio semplice e chiaro se i dati potranno essere riutilizzati da terzi e in tal caso per quali scopi (cfr. paragrafo 3.7 del Parere 02/2013, sulle applicazioni per dispositivi intelligenti adottato il 27 febbraio 2013).

Tenuto conto che tali piattaforme sono principalmente accessibili tramite un sito *internet* e che i trattamenti effettuati mediante le stesse perseguono

molteplici finalità, è raccomandato l'uso di informative stratificate o progressive, che consentano agli utenti di consultare le specifiche sezioni di interesse.

In termini pratici, tenuto conto delle richiamate tre macro tipologie di trattamento svolte attraverso le piattaforme, si sottolinea l'importanza che tra le informazioni da rendere agli interessati siano chiaramente rappresentati gli elementi che seguono.

1. Trattamenti dei dati personali degli utenti che si registrano sulle piattaforme, è importante che siano chiaramente 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, in particolare, 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).
2. Trattamenti dei dati personali dei professionisti sanitari:
    - 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, tra cui i tempi di conservazione, avendo cura di specificare:
        - i 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;
        - eventuali trattamenti in ordine ai giudizi di gradimento espressi dal paziente sul professionista sanitario.

3. Trattamenti di dati sulla salute dei pazienti -che potrebbero essere venuti in contatto con il professionista sanitario attraverso la piattaforma- in occasione, ad esempio della prenotazione di una visita specialistica, eventualmente effettuati dal predetto professionista per finalità di cura, in qualità di titolare, è necessario 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 predetti medici.

8. Trattamenti effettuati al di fuori del territorio nazionale

Dalle istruttorie condotte da questa Autorità è emerso che le piattaforme in esame, nella maggior parte dei casi, sono gestite da soggetti non sempre stabiliti in Italia. Il trattamento svolto può pertanto assumere la natura di trattamento transfrontaliero, definito dal Regolamento quale:

"*a) il trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure*

b) il trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro"[3] (art. 4(23) del Regolamento).

In caso di trattamento transfrontaliero, 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 (definite, in questo caso, "autorità interessate") per quanto riguarda i "*trattamenti transfrontalieri*" di dati personali svolti da tali titolari o responsabili.

L'obiettivo della devoluzione di competenze a favore dell'autorità capofila è quello di garantire l'esistenza di uno "*sportello unico*" per i trattamenti transfrontalieri di dati personali. Infatti, "*l'autorità di controllo capofila è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale titolare o responsabile*" (art. 56, par. 6, del Regolamento), fatte salve alcune eccezioni come quelle previste dall'art. 56, par. 2 del Regolamento in base al quale: "*In deroga al paragrafo 1, ogni autorità di controllo è competente per la gestione dei reclami a essa proposti o di eventuali violazioni del presente regolamento se l'oggetto riguarda unicamente uno stabilimento nel suo Stato membro o incide in modo sostanziale sugli interessati unicamente nel suo Stato membro*".

A tale riguardo, la natura transfrontaliera del trattamento deve essere portata a conoscenza degli interessati prima che il trattamento abbia inizio, assieme agli elementi indicati al precedente punto 7); ciò al fine di renderli edotti della circostanza che la presentazione del reclamo presso altre Autorità

[3] Art. 4 (16) del Regolamento definisce lo «stabilimento principale»:
a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

(c.d. Autorità interessata), comporta da parte di quest'ultima l'avvio della procedura di cooperazione tra l'Autorità di controllo capofila e le altre Autorità interessate, ai sensi dell'art. 60 del Regolamento (cfr. Linee guida 8/2022 sull'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento Versione 2.0, Adottate il 28 marzo 2023").

Qualora, il trattamento coinvolga anche soggetti stabili presso paesi terzi, si applicano le specifiche disposizioni di cui agli artt. 45 e seguenti del Regolamento e si rende necessario informare l'interessato di tali operazioni, avendo cura di evidenziare il presupposto legittimante il predetto trasferimento e le garanzie adeguate che si intendono prevedere.

9. Il principio di *Privacy by design*

L'art. 25, par. 1, del Regolamento prevede che "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento [debba mettere] in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*".

In base al principio della "*protezione dei dati fin dalla progettazione*", il titolare del trattamento è tenuto, pertanto, ad attuare i principi di protezione dei dati (art. 5 del Regolamento) adottando misure tecniche e organizzative adeguate e integrando nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati.

Il Considerando 78 del Regolamento (cfr. EDPB - Linee Guida 4/2019 Data Protection by Design and by Default) prevede che "*in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili*

del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici".

Il considerando 78 del Regolamento evidenzia una responsabilità dei titolari, ossia quella di valutare costantemente se stiano utilizzando, in qualunque momento, mezzi appropriati di trattamento e se le misure scelte contrastino effettivamente le vulnerabilità rilevate. Inoltre, i titolari dovrebbero effettuare revisioni periodiche delle misure di sicurezza poste a presidio e tutela dei dati personali, nonché della procedura per la gestione delle violazioni dei dati ai sensi degli artt. 33 e 34 del Regolamento.

Il principio di *"privacy by design*" ha dunque lo scopo di garantire l'esistenza di un corretto livello di protezione dei dati personali fin dalla fase di progettazione (design) di qualunque sistema, servizio, prodotto o processo così come durante il loro ciclo di vita al fine di attuare in modo efficace i principi di protezione dei dati personali (cfr. Sent. Cass. Dell'11 ottobre 2023, n. 28385).

Queste misure potranno comprendere diverse soluzioni: sia avanzate e di natura tecnologica, come l'uso di sistemi di codifica; sia organizzative come la formazione del personale. In ogni caso, il titolare, nell'implementazione di tali misure, deve tenere conto di alcuni elementi imprescindibili, quali: il contesto in cui si svolge il trattamento; la natura dei dati trattati; le finalità del trattamento; la natura transfrontaliera del trattamento; i potenziali rischi in materia di diritti e libertà degli interessati; lo stato dell'arte tecnologico; i costi di attuazione, sia in termini temporali che di risorse umane.

A tale riguardo, si evidenzia altresì che i produttori di prodotti, servizi e applicazioni – come evidenziato dalle citate "*Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita*", rappresentano, insieme ai responsabili del trattamento, figure essenziali ai fini della protezione dei dati fin dalla progettazione e per impostazione predefinita e dovrebbero essere consapevoli del fatto che i titolari del trattamento sono tenuti a trattare i dati personali solo utilizzando sistemi e tecnologie che integrano by design e by default i principi di protezione dei dati (cfr. considerando 78 del Regolamento e punto 94 delle citate Linee guida).

10. La sicurezza del trattamento

Il Regolamento prevede che il titolare del trattamento metta in atto "*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*", tenendo conto, tra l'altro, "*della natura, dell'oggetto, del contesto e delle finalità del trattamento, come 7 anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*" e che "*nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati*" (art. 32 del Regolamento).

Con riferimento ai trattamenti in esame, il titolare deve porre particolare attenzione ad 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.

Sulla base del principio di integrità e riservatezza, l'art. 32 del Regolamento prevede che il titolare del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, debba mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso, "*la cifratura dei dati personali*".

Allo stato dell'arte, l'utilizzo di tecniche crittografiche è una delle misure più comunemente adottate per proteggere, in particolar modo, i dati personali degli utenti di un servizio *on-line* durante la loro trasmissione su rete Internet. Al riguardo, si richiama l'attenzione sulla scelta di un protocollo di rete che garantisca la riservatezza e l'integrità dei dati scambiati tra il *browser* dell'utente e il *server* che ospita i servizi delle predette piattaforme, consentendo inoltre agli utenti di verificare l'autenticità del sito *web* visualizzato.

I proprietari/gestori delle piattaforme dovranno inoltre prevedere a titolo esemplificativo e non esaustivo le seguenti misure:

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.

Si ricorda infine che eventuali *cookies* e altri strumenti di tracciamento non strettamente necessari alla fornitura del servizio possono essere utilizzati, a condizione che l'utente abbia espresso il proprio consenso e sia stato adeguatamente informato (cfr. Linee guida *Cookie* e altri strumenti di tracciamento - 10 giugno 2021, doc. *web* n. 9677876).