


# Proposta di revisione della normativa privacy in sanità.



## PREMESSA

La digitalizzazione dei sistemi sanitari ha cambiato radicalmente il modo di trattare i dati sanitari (DS), che sono diventati una risorsa fondamentale per la programmazione, la prevenzione e la cura delle malattie. Gli Open Data, ovvero i dati aperti e accessibili a tutti, stanno guadagnando sempre più importanza e ogni Paese sta creando il suo Registro Dati Sanitari, una banca dati nazionale che raccoglie le informazioni sanitarie di tutti i residenti.


Per sfruttare al meglio i dati sanitari, è necessario utilizzare strumenti avanzati, come la stratificazione e l'interconnessione dei flussi sanitari. La stratificazione consiste nell'usare algoritmi predittivi per classificare la popolazione in base al profilo di rischio, al bisogno di salute e al consumo di risorse. In questo modo, si possono adottare strategie di intervento differenziate e personalizzate per ogni assistito. Un esempio di applicazione della stratificazione è l'oncologia territoriale, che ha bisogno di identificare e coinvolgere i *non responders* agli screening per prevenire e curare i tumori.

La condivisione dei dati sanitari tra settori e Paesi richiede però una *governance* adeguata, che garantisca la sicurezza, la privacy e la qualità dei dati. Il Data Governance Act - DGA (applicato dal 24 settembre 2023) promuove la condivisione dei dati e mira a costruire un ambiente affidabile, facilitando la ricerca innovativa e la produzione di prodotti e servizi innovativi. Il DGA promuove l'altruismo dei dati in tutta l'UE, rendendo più facile per i singoli e le aziende rendere volontariamente disponibili i propri dati per il bene comune, ad esempio per i progetti di ricerca medica. In parallelo, la UE si sta avvicinando all'adozione, su proposta della Commissione, di un Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS), che dovrebbe condurre alla piena realizzazione del fascicolo sanitario elettronico europeo e alla valorizzazione secondaria dei dati sanitari, nel rispetto della privacy, per finalità di governo e di ricerca.

In Italia, il Codice dell'Amministrazione Digitale (CAD) stabilisce che lo Stato, le Regioni e le autonomie locali devono assicurare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale, utilizzando le tecnologie più appropriate e soddisfacendo gli interessi degli utenti. Il trattamento dei dati sanitari da parte delle Regioni e delle ASL è regolato sia dalla normativa sulla protezione dei dati personali, sia da quella sanitaria, non sufficientemente coordinate fra loro. L'uso dei dati per la profilazione sanitaria si rivelerebbe uno strumento essenziale per la programmazione, la prevenzione e per la gestione più efficace dei bisogni dei pazienti, anticipando le necessità e riducendo il carico di malattia e di risorse.

In questo quadro, la circolazione dei dati sanitari per finalità di prevenzione e programmazione sanitaria - oltre che di cura - sul territorio nazionale risulta ancora difficoltosa. Queste barriere devono essere superate per realizzare la Mission 6 del PNRR, che prevede il potenziamento delle reti di assistenza di prossimità, e il DM 77/2022, che ne disciplina l'attuazione. Il consenso

# Proposta di revisione della normativa privacy in sanità.




dell'interessato, che è ancora il principale presupposto per il trattamento dei dati relativi alla salute per finalità di ricerca, potrebbe essere rivisto o integrato con altre basi giuridiche, per favorire la condivisione dei dati e la collaborazione tra i ricercatori in ambito sanitario.

In definitiva, la digitalizzazione dei sistemi sanitari e la *governance* dei dati sono due temi cruciali e interconnessi, che richiedono una costante attenzione e un continuo aggiornamento da parte di tutti gli attori coinvolti, per garantire, da un lato, il rispetto dei diritti e delle preferenze dei cittadini e, dall'altro, per promuovere la salute e l'innovazione nel segno della sostenibilità.

## PROPOSTA


1. Politiche europee: si porta in evidenza lo sforzo delle Istituzioni dell'Unione Europea finalizzato alla creazione di uno spazio europeo dei dati sanitari. In particolare, la proposta di Regolamento sullo European Health Data Space intende rafforzare il controllo del paziente sui propri dati sanitari e favorirne l'uso secondario a fini non solo di erogazione dell'assistenza sanitaria, ma anche di ricerca, innovazione ed elaborazione delle politiche sanitarie. Ulteriori regolamenti europei, come i Data Governance Act, il Data ACT, l'AI ACT, possono rivelarsi – se ben attuati – strumenti di salvaguardia delle persone e dei loro dati sanitari, consentendone, al contempo, il buon uso per il miglioramento delle performance dei Servizi Sanitari.
2. Il trattamento dei dati relativi alla salute per finalità di ricerca medica, biomedica ed epidemiologica, secondo la normativa italiana (art. 110 del Codice Privacy) può essere effettuato sulla base del consenso dell'interessato oppure, ove informare l'interessato risulti impossibile o implichi uno sforzo sproporzionato, previa consultazione preventiva del Garante per la protezione dei dati personali, ai sensi dell'articolo 36 del GDPR. Tale situazione rende difficoltosa la ricerca, specie per i casi di studi osservazionali retrospettivi, e non tiene conto dell'orientamento della ricerca verso i principi dell'*Open Science* e della condivisione dei risultati e dei dati di ricerca. Si auspica, dunque, una revisione dell'attuale normativa che, in conformità agli orientamenti espressi dall'Unione Europea e dallo stesso Comitato Europeo per la Protezione dei Dati, consenta di fondare la ricerca scientifica su altre basi giuridiche; in particolare, tra esse, la necessità di esecuzione di un compito di interesse pubblico, come previsto dall'art. 6, paragrafo 1, lettera e) GDPR - nel caso in cui l'esecuzione delle sperimentazioni cliniche rientri direttamente nel mandato, nelle funzioni e nei compiti assegnati ex lege ad un organismo pubblico o privato - o il legittimo interesse di cui all'art. 6, paragrafo 1, lettera f) GDPR, in combinato disposto, per le categorie particolari di dati come quelli sulla salute, con i motivi di interesse pubblico nel settore della sanità pubblica, ai sensi dell'art. 9, paragrafo 2, lettera i) ovvero le finalità di ricerca scientifica ai sensi dell'art. 89, paragrafo 1 (art. 9, paragrafo 2, lettera j) GDPR.

# Proposta di revisione della normativa privacy in sanità.



3. In generale, in ottica di sostenibilità, dovrebbe essere facilitato l'uso secondario dei dati per finalità ulteriori rispetto a quelle per cui i dati sono originariamente raccolti, accompagnando tale apertura con attività di sensibilizzazione in merito al rispetto dei diritti fondamentali e a una corretta gestione del dato, incluso l'uso di tecniche di minimizzazione e anonimizzazione dei dati personali.
4. Titolari del trattamento dati, circolarità e accesso ai dati personali: i diversi soggetti coinvolti nel percorso di cura di un paziente devono essere facilitati nell'accesso ai dati di interesse utili a gestire il caso. Garantire la sicurezza significa garantire confidenzialità, integrità ma anche disponibilità dei dati: dati integri ma inaccessibili possono determinare ritardi nelle cure e sospensioni di processi critici così come duplicazioni nella raccolta di dati, che possono degradare la qualità delle informazioni o determinare incongruenze, riducendo così anche il livello complessivo di integrità e confidenzialità del dato. In questo contesto diventa indispensabile, quindi, impostare un approccio di HTA, che miri all'integrazione dei dati sanitari con i dati non sanitari (es. socioeconomici) per poter attuare una reale presa in carico sociosanitaria dell'assistito e per favorire una programmazione sanitaria che tenga conto dei bisogni socioassistenziali del singolo. Ovviamente, tutto ciò deve prevedere una definizione chiara di compiti e responsabilità privacy (ai sensi del GDPR) e devono essere individuati i soggetti autorizzati ad accedere ai dati ed i diversi profili di autorizzazione, in linea con il principio di minimizzazione.
5. Il GDPR ha introdotto per la disciplina della protezione dei dati personali un concetto maturo in altre discipline: il principio di *accountability* (o responsabilizzazione) delineato dagli articoli 5 e 24 del GDPR, che richiede al titolare di mettere in atto misure tecniche ed organizzative adeguate a garantire - ed essere in grado di dimostrare - che il trattamento sia svolto conformemente al Regolamento UE. Tale valutazione deve essere fatta *"tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche"*. SIMM intende promuovere il cambio di mentalità nella gestione della privacy in sanità che sia incentrata sull'*accountability* e sulla piena consapevolezza di tale principio.
6. Stakeholders: i principali stakeholders istituzionali e scientifici devono farsi portavoce presso le Istituzioni, in articolare il Ministero della Salute e il Garante Privacy, delle problematiche connesse ad un'applicazione del GDPR troppo restrittivo, ma devono anche portare proposte di principio e concrete per il superamento di vincoli che, di fatto, limitano la capacità di azione delle articolazioni del SSN.
7. Digitalizzazione: qualsiasi processo può e deve essere pensato *"digital first"*, non per escludere chi non sia in grado di utilizzare correttamente la tecnologia, ma perché sistemi ben progettati possono diffondere una raccolta delle informazioni capillare e controllata.

# Proposta di revisione della normativa privacy in sanità.



- Inoltre, possono supportare raccolte di informazioni non digitali fornendo guide o indicazioni operative associate alla conformazione fisica dei servizi sanitari nel territorio di riferimento.
8. La medicina d’iniziativa è lo strumento che potrebbe diventare parte integrante della cura, come previsto in numerosi atti di programmazione del SSN. Si auspica un chiarimento del quadro normativo relativo alla medicina di iniziativa e, insieme, un superamento della necessità del consenso dell’interessato (attualmente richiesto dal Garante per la protezione dei dati personali, *legibus sic stantibus*), in ottica di facilitazione del ricorso a tale strumento e di bilanciamento con il fine rilevante del miglioramento della salute pubblica.
  9. DPO e Comitato Etico: allo scopo di perseguire le finalità descritte nei punti 2, 3 e 4 (almeno), è opportuno che il Data Protection Officer possa mantenere un canale di comunicazione costante e aperto con il Comitato Etico e il Comitato Etico introduca al suo interno competenze orientate a valutare al meglio i nuovi paradigmi che abilitano alla valorizzazione di Big Data e Intelligenza Artificiale; si tratta di strumenti di grande potenza informativa, che, tuttavia, comportano un incremento di complessità e conseguenze in termini di fattibilità, sostenibilità e tutela dei diritti delle persone.
  10. FAIR e Open Data: è necessario promuovere il ricorso ai principi FAIR (*findability, accessibility, interoperability, reusability*) e alle logiche Open Data (accesso generalizzato e libero uso) nei processi di raccolta, pseudonimizzazione, sintetizzazione e trasformazione in forma anonima dei dati personali, anche per dare piena attuazione alle potenzialità del Data Governance Act e degli Spazi Europei dei Dati.