Co-funded by the
European Union

Il trattamento dei dati sanitari alla luce del Regolamento Generale sulla Protezione dei Dati (*General Data Protection Regulation* - GDPR)

La proposta di Regolamento UE sul nuovo *European Health Data Space* (EHDS)

agostina.latino@unicam.it

Premessa: di cosa parliamo quando parliamo di dati

Sono **dati personali** le informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

Particolarmente importanti sono:

- i **dati che permettono l'identificazione diretta:** dati anagrafici (ad es.: nome e cognome), le immagini, ecc.
- i **dati che permettono l'identificazione indiretta:** numero di identificazione (ad es.: il codice fiscale, l'indirizzo IP, il numero di targa);
- i **dati rientranti in particolari categorie**: si tratta dei dati c.d. **sensibili**, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il **Regolamento (UE) 2016/679** (art. 9) ha incluso nella nozione anche i **dati genetici,** i **dati biometrici** e quelli relativi all'**orientamento sessuale**;
- i **dati relativi a condanne penali e reati**: si tratta dei dati c.d. **giudiziari**, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il **Regolamento (UE) 2016/679** (art. 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie, **altri dati personali** hanno assunto un ruolo significativo, come **quelli relativi alle comunicazioni elettroniche** (via Internet o telefono) e **quelli che consentono la geolocalizzazione**, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

Nozione di «dato sensibile»

La Convenzione del Consiglio d'Europa sulla *protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, adottata a Strasburgo il 28 gennaio 1981, n. 108, chiarisce la nozione di «dato sensibile» all'art. 6, disponendo che «i dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i **dati a carattere personale relativi alla salute** o alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno preveda delle garanzie appropriate. Lo stesso vale per i dati a carattere personale relativi a condanne penali».

Questa norma era in pratica mutuata dall'art. 8 (**Trattamenti riguardanti categorie particolari di dati**) della Direttiva n. 46 del 1995 (**Sulla protezione dei dati personali**), base giuridica, in Italia, del D.lgs. 196/2003 ("Codice in materia di protezione dei dati personali", c.d. **Codice privacy**) che faceva perno sul consenso dell'interessato.

L'art. 9, par. 2, la Convenzione previde possibilità di deroga quando essa:

«è prevista dalla legge della Parte e costituisce una misura necessaria, in una società democratica:

a) per la protezione della sicurezza dello Stato, per la sicurezza pubblica, per gli interessi monetari dello Stato o per la repressione dei reati;

b) per la protezione della persona interessata e dei diritti e delle libertà di altri».

Art. 26 del previgente Codice privacy

- L'art. 26.1 del previgente Codice privacy prevedeva che i dati sensibili (di cui i dati sanitari erano parte) potevano essere **oggetto di trattamento solo con il consenso dell'interessato e previa autorizzazione del Garante**.
- Il successivo comma 4 prevedeva una serie di casi particolari in cui il trattamento dei dati sanitari era ammesso anche senza consenso, ferma restando la necessità della previa autorizzazione del Garante.
- In particolare, per quanto riguarda i dati relativi alla salute, la lett. b) faceva riferimento all'ipotesi in cui il trattamento dei dati fosse **necessario** per la salvaguardia della vita o dell'incolumità fisica di **un terzo**.
- Se invece la stessa esigenza si poneva con riferimento all'interessato, e questo non era in grado di prestare il consenso per impossibilità fisica, incapacità di agire o incapacità di intendere e di volere, era previsto che *"il consenso è manifestato da chi esercita legalmente la* **potestà**, *ovvero da un* **prossimo congiunto**, *da un* **familiare**, *da un* **convivente** *o, in loro assenza, dal* **responsabile della struttura** *presso cui dimora l'interessato".*

Art. 82 del previgente Codice privacy

Nella stessa ottica l'art. 82 del Codice dettava una disciplina specifica per le situazioni di emergenza, prevedendo che l'informativa e il consenso al trattamento dei dati personali potevano intervenire *"senza ritardo, successivamente alla prestazione"* quando sussisteva una delle seguenti ipotesi:

1. **impossibilità fisica**, **incapacità di agire o incapacità di intendere e di volere dell'interessato**, quando non è possibile acquisire il consenso dai soggetti indicati dalla lett. b) dell'art. 26;
2. **rischio grave, imminente e irreparabile** per la salute o l'incolumità fisica dell'interessato;
3. **prestazione medica** che può essere pregiudicata dall'acquisizione preventiva del consenso, in termini di **tempestività o efficacia**.

Il quadro che emergeva dal combinato disposto di questi articoli dimostrava che, di fatto, nel sistema codicistico **non esistevano casi in cui il trattamento di dati sanitari per finalità di cura dell'interessato potesse prescindere dal rilascio di un consenso** (preventivo o successivo, proveniente direttamente dall'interessato o da un terzo, ma comunque sempre necessario).

D'altra parte, il Codice non contemplava l'ipotesi in cui l'interessato, pur richiedendo una prestazione sanitaria necessaria per la tutela della sua vita o incolumità fisica, rifiutasse di prestare il consenso al trattamento dei suoi dati personali.

Nel sistema delineato dal Codice in questo caso, a rigore, il medico avrebbe dovuto rifiutarsi di eseguire la prestazione, e il tema diveniva ancora più complesso nel caso in cui il medico avesse già effettuato la prestazione senza richiedere alcun consenso, per la sussistenza di una delle ipotesi di cui all'art. 82, ma successivamente l'interessato avesse rifiutato di rilasciare il proprio consenso. In questo caso il medico che era intervenuto tempestivamente per salvaguardare l'incolumità dell'interessato avrebbe rischiato di essere chiamato a rispondere per avere trattato illecitamente i dati personali di quest'ultimo.

Nozione di «dato sensibile»

Il 18 maggio 2018 il Consiglio d'Europa ha adottato il Protocollo di emendamento alla Convenzione sulla *protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, avvicinando la Convenzione alla disciplina del reg. Ue n. 679/2016. L'Italia ne ha autorizzato la ratifica con legge 22 aprile 2021, n. 60, e ne ha ordinato l'esecuzione.

Le modifiche prospettate comprendono il testo dell'art. 6 della Convenzione, che viene sostituito dal seguente:

«1. L'elaborazione di:

- dati genetici;
- dati personali relativi a infrazioni, procedimenti e condanne penali e misure di sicurezza;
- dati biometrici che identificano in modo univoco una persona;
- dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, l'appartenenza sindacale, la religione o altre convinzioni, la salute o la vita sessuale,

sono consentiti solo se sono previste **garanzie di legge**, a complemento di quelle della presente Convenzione.

2. Tali garanzie tutelano contro i rischi che il trattamento di dati sensibili può presentare per gli interessi, i diritti e le libertà fondamentali dell'interessato, in particolare un rischio di discriminazione».

Sistemi sanitari e dati

Un sistema sanitario sicuro, efficiente e sostenibile dipende fortemente dai dati.

I dati possono:

- supportare il processo decisionale clinico,
- consentire la pianificazione, la supervisione e il miglioramento del sistema sanitario,
- fornire informazioni che consentano ai pazienti di impegnarsi attivamente nella gestione della propria salute e del proprio benessere.

Nozione di «dato sanitario»

I dati includono:

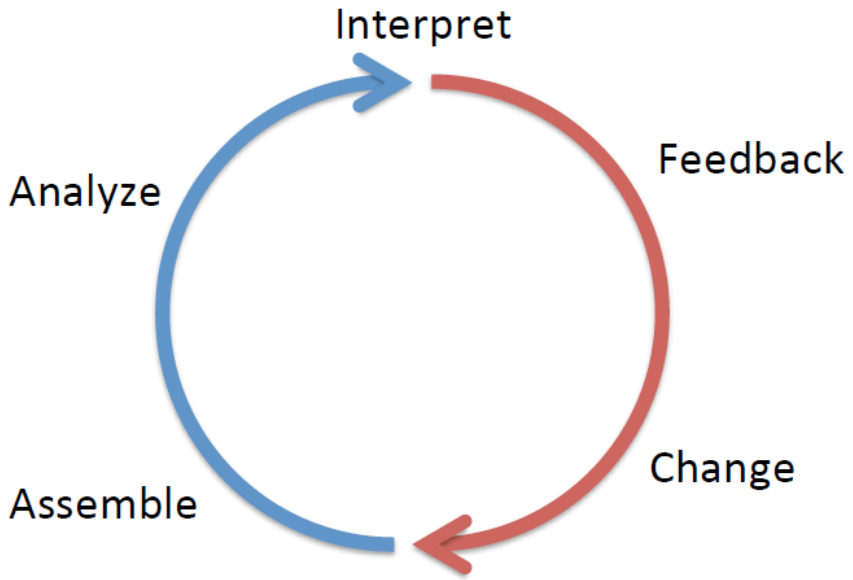
- dati formalmente strutturati nelle cartelle cliniche elettroniche
- immagini mediche
- prescrizioni di farmaci
- rapporti di laboratorio
- dati sulle richieste di rimborso
- esiti riportati dai pazienti
- altri strumenti di gestione dei dati utilizzati all'interno dei sistemi sanitari

Comprendono anche dati generati al di fuori dell'ambiente sanitario, come quelli provenienti da dispositivi per il benessere come i *fitness tracker*

Sistema sanitario di apprendimento

Principio *FAIRness* dei dati:

- ***Findable*** (reperibili)
- ***Accessible*** (accessibili)
- ***Interoperable*** (interoperabili)
- ***Reusable*** (riutilizzabili)



Dati sanitari e pandemia

COVID-19 e condivisione dei dati:

- segnalazione dell'incidenza della malattia da parte della sanità pubblica e della tracciabilità dei contatti
- necessità di dati accessibili per la ricerca collaborativa in molti Paesi, sia all'interno che all'esterno dell'UE
- valutazione degli effetti dei trattamenti e dei vaccini

L'attenzione per una migliore disponibilità e accessibilità dei dati era tuttavia già evidente nella politica dell'UE prima di essere acuita dalla crisi COVID-19, e costituisce la base di una delle priorità stabilite nel mandato della Commissione di sviluppare uno Spazio europeo dei dati sanitari (*European Health Data Space* -EHDS; come descritto nella comunicazione della Commissione "Una strategia europea per i dati"; COM 2020a).

European Health Data Space

EHDS: non mero *database*, bensì:

sistema per lo scambio e l'accesso ai dati regolato da norme, procedure e standard tecnici comuni per garantire l'accesso ai dati sanitari all'interno degli Stati membri e tra di essi, nel pieno rispetto dei diritti fondamentali delle persone, in linea con il Regolamento generale sulla protezione dei dati (GDPR) e le competenze degli Stati membri.

Obiettivi:

- rafforzare ed estendere l'uso e il riutilizzo dei dati sanitari ai fini della ricerca e dell'innovazione nel settore sanitario;
- aiutare le autorità sanitarie a prendere decisioni basate su dati concreti;
- migliorare l'accessibilità, l'efficacia e la sostenibilità dei sistemi sanitari;
- sostenere il lavoro degli enti normativi nella valutazione dei prodotti medici e nella dimostrazione della loro sicurezza, efficacia e qualità;
- contribuire alla competitività dell'industria dell'UE.

L'EHDS fornirà l'accesso ai set di dati necessari per utilizzare con successo le tecniche emergenti di intelligenza artificiale responsabile e incentrata sull'uomo e di apprendimento automatico per promuovere l'innovazione nell'assistenza sanitaria.

Il GDPR come punto di partenza

Il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. GDPR, *General Data Protection Regulation*), che abroga la direttiva 95/46/CE, è divenuto applicabile in tutti gli Stati membri a partire dal 25 maggio 2018.

Gli obiettivi del GDPR (art. 1) sono due:

1. ***facilitare la libera circolazione dei dati personali***, compreso lo scambio transfrontaliero
2. ***tutelare i diritti e le libertà fondamentali*** delle persone fisiche in materia di ***privacy*** e protezione dei ***dati personali***

Definizione di «dati relativi alla salute»

Il Regolamento introduce per la prima volta una definizione di “dati relativi alla salute”, secondo cui tali dati consistono ne «**i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute**» (art. 4, par. 15).

Nella pratica, tuttavia, i dati sanitari sono spesso intesi come qualsiasi dato personale generato all'interno dei sistemi sanitari, e alcuni possono anche includere dati relativi alla salute raccolti da cittadini e pazienti attraverso dispositivi indossabili, app e informazioni autodichiarate.

Il considerando n. 35 del Regolamento precisa inoltre 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».

Agli Stati membri è stato consentito, attraverso clausole di specificazione, di adattare l'applicazione di alcuni aspetti del Regolamento alla loro situazione nazionale.

Il Regolamento non esclude le leggi degli Stati membri preesistenti o di recente adozione che stabiliscono circostanze per il trattamento specifico di categorie particolari di dati nell'interesse pubblico.

Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese le limitazioni relative al trattamento, tra l'altro, di dati relativi alla salute (art. 9(4) GDPR).

Art. 9 GDPR: “Trattamento di categorie particolari di dati personali”

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, **dati relativi alla salute o alla vita sessuale o all'orientamento sessuale** della persona.

Art. 9 GDPR: “Trattamento di categorie particolari di dati personali”

2. Il paragrafo 1 **non si applica** se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio **consenso esplicito** al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al par. 1;

b) il trattamento è **necessario** per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di **diritto del lavoro e della sicurezza sociale e protezione sociale**, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un **interesse vitale** dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

Art. 9 GDPR: “Trattamento di categorie particolari di dati personali”

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua **finalità politiche, filosofiche, religiose o sindacali**, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi **manifestamente pubblici** dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in **sede giudiziaria** o ogniqualvolta le autorità giurisdizionali esercitino le loro **funzioni giurisdizionali**;

Art. 9 GDPR: “Trattamento di categorie particolari di dati personali”

g) il trattamento è necessario per motivi di **interesse pubblico** rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di **medicina preventiva** o di **medicina del lavoro**, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di **interesse pubblico nel settore della sanità pubblica,** quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di **archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici** in conformità dell'art. 89, par. 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Art. 9 GDPR: “Trattamento di categorie particolari di dati personali”

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti. (c.d. eccezione per finalità di cura, ndr)

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Art. 9 GDPR quale «principio generale»

La peculiare posizione dell'art. 9 GDPR, ossia nei principi generali, idealmente all'apice del Regolamento, suggerisce la rilevanza e il valore di quanto esso dispone, ciò che deve rispecchiarsi nell'interpretazione e applicazione delle regole successive, anche di dettaglio, quasi avesse valenza, per così dire, “para-costituzionale”.

Va dunque letto in armonia con l'art. 5 GDPR, il quale sancisce appunto i principi applicabili al trattamento di dati personali, che irradiano e informano l'intera regolamentazione in materia:

liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione.

I principi posti a base del trattamento dei dati personali nel settore sanitario

liceità, correttezza e trasparenza – i dati devono essere trattati in modo legale, corretto e trasparente nei confronti del paziente;

limitazione della finalità – i dati devono essere raccolti solo per scopi specifici, legittimi e successivamente trattati in modo coerente con tali scopi;

minimizzazione dei dati – i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto agli scopi del trattamento;

esattezza – dati devono essere accurati e aggiornati o modificati quando necessario, al verificarsi un loro cambiamento;

limitazione della conservazione – i dati devono essere conservati solo per un periodo limitato, non oltre quanto necessario per gli scopi del trattamento;

integrità e riservatezza – deve essere garantita la sicurezza dei dati con misure tecniche e organizzative adeguate a prevenire accessi non autorizzati o perdite;

responsabilizzazione – il titolare del trattamento deve essere in grado di dimostrare la conformità ai suddetti principi.

Art 9 GDPR fra regola e eccezioni

L'art. 9 GDPR al par. 1 pone un divieto generale di trattare i dati sensibili ma tale divieto viene derogato dal successivo par. 2 che ne ammette il trattamento purché sussista almeno una delle 10 condizioni elencate nel medesimo paragrafo.

Inoltre, il par. 4 dell'art. 9 riconosce agli Stati membri la possibilità di mantenere o introdurre ulteriori condizioni, comprese limitazioni, per il trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Rimane quindi aperta la possibilità, per il legislatore nazionale, di introdurre condizioni più stringenti volte a garantire un livello di tutela più elevato di quello derivante dalla disciplina del Regolamento. In ogni caso, in assenza di tale intervento, a partire dal 25 maggio 2018 (data della definitiva applicabilità del GDPR) la necessità di diagnosi, assistenza o terapia sanitaria o sociale, o la necessità per motivi di interesse pubblico nel settore della sanità pubblica, configurano condizioni sufficienti per permettere il trattamento dei dati sanitari dei pazienti, senza bisogno di acquisire il consenso degli stessi.

NB: il consenso dell'interessato figura solo come una delle possibili condizioni, ponendosi sullo stesso piano delle altre alternative previste.

Art. 6 GDPR: Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è **necessario** all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è **necessario** per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è **necessario** per la salvaguardia degli **interessi vitali** dell'interessato o di un'altra persona fisica;

e) il trattamento è **necessario** per l'esecuzione di un compito di **interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è **necessario** per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Consenso

- L'art. 4 n. 11 del GDPR definisce il consenso dell'interessato come “qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato […]”.
- Come sottolineato anche dal Gruppo di Lavoro ex art. 29 nelle *Guidelines on Consent under Regulation 2016/679* (WP 259), il consenso si caratterizza, tra le altre cose, per essere “libero”, ovvero per presupporre una scelta e un controllo effettivi da parte dell'interessato.
- Il considerando 42 precisa che il consenso non può essere considerato liberamente espresso, e quindi valido, se l'interessato non può operare una scelta effettivamente libera o se non può rifiutare di prestare il proprio consenso senza subire pregiudizi.
- L'art. 7.4 aggiunge che nel valutare se il consenso è stato liberamente prestato si deve considerare in particolare se la prestazione del consenso sia una condizione essenziale per l'esecuzione della prestazione.
- Questo significa che se dal rifiuto del consenso possono derivare conseguenze significativamente negative per l'interessato, quali, in particolare, l'impossibilità di usufruire del servizio o di ricevere la prestazione richiesta, è evidente che il soggetto che ha interesse o bisogno di ricevere quella prestazione non gode di fatto di una libertà di scelta.
- Ne deriva che il consenso non è libero e, quindi, non può essere considerato valido come base giuridica del trattamento.

Consenso trattamento di dati personali per l'esecuzione di un trattamento sanitario

- Con riferimento al consenso al trattamento di dati personali per l'esecuzione di un trattamento sanitario, è evidente che tale consenso non può che essere necessario in quanto un professionista sanitario non potrebbe mai trattare, sul piano sanitario, un paziente, senza trattare anche i suoi dati personali.
- Il professionista dovrà infatti necessariamente venire a conoscenza di una serie di dati identificativi e clinici (es. anamnesi, stato di salute, farmaci assunti) e, d'altra parte, egli stesso, nel trattare il paziente, andrà a produrre una serie di dati relativi alla salute di quest'ultimo (es. lastre, referti, fogli chirurgici, ecc.).
- Dal momento che anche la semplice raccolta e consultazione dei dati costituisce un trattamento, è evidente che il medico, nello svolgimento delle sue funzioni, tratta costantemente e inevitabilmente i dati personali dei pazienti. Il consenso al trattamento dei dati sanitari diventa quindi “obbligatorio” proprio perché senza di esso il medico dovrebbe rifiutarsi di eseguire la prestazione medica, sicché si ha una sorta di ossimoro giuridico (come già detto, il consenso per essere effettivo deve sempre essere libero).
- Di fatto dunque il consenso sarà necessario per tutte le attività diverse da quelle connesse alle finalità di cura, come la consegna di referti online, l'uso di app mediche, la trasmissione di referti e ricette a terzi o la consultazione del fascicolo sanitario elettronico.

Trattamento dei dati sanitari: il decreto 101/2018

- In Italia, il 19 settembre 2018, è entrato in vigore il Decreto legislativo 10 agosto 2018, n. 101 recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679-GDPR (c.d. decreto di adeguamento).
- Tale decreto ha confermato l'impostazione del Regolamento con riferimento sia alle 6 basi giuridiche del trattamento, sia alle 10 condizioni per il trattamento delle categorie particolari di dati personali, confermando così la possibilità di trattare i dati relativi alla salute anche senza il consenso dell'interessato.

- Il decreto infatti abroga l'intero Titolo III della Parte I del Codice contenente i principi e le regole generali per il trattamento dei dati personali e aggiunge al Titolo I, *inter alia*, l'art. 2-septies che conferma che “i dati genetici, biometrici e relativi alla salute possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo [art. 9] e in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo”. Nei commi successivi dello stesso articolo si prevede infatti l'adozione, da parte del Garante, di un provvedimento che stabilisca le misure di garanzia per il trattamento dei dati in oggetto, in conformità a quanto previsto dal paragrafo 4 dell'art. 9 del GDPR.
- Con riferimento alla Parte II del Titolo V del Codice, rubricato “Trattamento di dati personali in ambito sanitario”, il decreto ha modificato l'art. 75 prevedendo che “il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del Regolamento, dell'articolo 2-septles del presente codice […]”.
- È stato inoltre modificato l'art. 77, relativo alle modalità particolari per trattare i dati personali e per fornire all'interessato le informazioni sul trattamento, in cui è stato eliminato il riferimento al consenso per il trattamento dei dati personali. Il decreto è poi intervenuto marginalmente sugli artt. 78, 79, 80 e 82, adeguandoli alle nuove disposizioni del GDPR ma lasciandoli invariati nel loro contenuto sostanziale, e ha invece abrogato gli artt. 76, 81, 83 e 84.

- Di particolare rilievo è stata l'abrogazione dell'art. 81 relativo alla “Prestazione del consenso” che prevedeva la possibilità di manifestare oralmente il consenso al trattamento dei dati idonei a rivelare lo stato di salute, con annotazione dell'esercente la professione sanitaria ai fini di documentare il rilascio del consenso. Tale abrogazione conferma dunque il venir meno della necessità di acquisire il consenso del paziente.
- Il decreto di adeguamento dimostra quindi l'intenzione del legislatore di adeguare in pieno la disciplina nazionale al Regolamento superando, anche con riferimento ai dati relativi alla salute, la precedente concezione basata sulla centralità del consenso.
- In ogni caso, indipendentemente dal decreto di adeguamento, a partire dal 25 maggio 2018 il Regolamento è definitivamente applicabile in tutti gli Stati membri, con conseguente automatica disapplicazione di tutte le norme nazionali con esso incompatibili.
- In effetti, la fonte normativa della nuova disciplina europea sul trattamento dei dati non è più una direttiva, come per la disciplina precedente su cui si basava il Codice privacy, bensì, appunto, un regolamento che, in quanto tale, non necessita di una legge nazionale di attuazione, ma è direttamente applicabile in tutti gli Stati membri.
- Questo significa che fin dal 25 maggio 2018, anche in mancanza del decreto di adeguamento, è divenuto possibile trattare per finalità mediche i dati relativi alla salute senza bisogno di acquisire il consenso del soggetto interessato, purché sussista una delle condizioni previste dal par. 2 dell'art. 9 del GDPR e il trattamento si fondi su una delle basi giuridiche di cui al par. 1 dell'art. 6 del GDPR.

Funzioni del trattamento dei dati sanitari

Funzione 1: trattamento dei dati ai fini della fornitura di **assistenza sanitaria e sociale** da parte di fornitori di servizi sanitari e di assistenza al paziente interessato. Ciò include sia l'assistenza di persona che la teleassistenza tramite strumenti di eHealth o mHealth

(ps: secondo l'OMS:

eHealth: «utilizzo delle tecnologie informatiche e di telecomunicazione in ambito sanitario».

mHealth: «pratica di assistenza sanitaria pubblica e medica supportata dai dispositivi mobili, come smartphone, dispositivi per il monitoraggio del paziente, assistenza digitale personalizzata e altri dispositivi wireless»).

Funzione 2: trattamento dei dati per finalità più ampie di **sanità pubblica**, tra cui la pianificazione, la gestione, l'amministrazione e il miglioramento dei sistemi sanitari e assistenziali; la prevenzione o il controllo delle malattie trasmissibili; la protezione da gravi minacce alla salute e la garanzia di elevati standard di qualità e sicurezza dell'assistenza sanitaria e dei prodotti e dispositivi medici.

Funzione 3: trattamento dei dati per la **ricerca scientifica o storica** da parte di organizzazioni del settore pubblico e privato (terze parti, che non sono il titolare originario dei dati), comprese le industrie farmaceutiche e di tecnologia medica e i fornitori di assicurazioni.

Funzione 1: uso primario

Riguarda i dati sanitari raccolti direttamente in relazione a un paziente nel contesto dell'assistenza sanitaria e sociale al fine di fornire servizi sanitari o di assistenza a quel paziente. Può essere necessario condividere tali dati oltre i confini dell'UE nel caso di pazienti che ricevono cure in uno Stato membro diverso da quello di residenza abituale.

Ciò può avvenire per le cure programmate e non programmate dei visitatori, per le cure non programmate dei residenti temporanei, per le cure programmate in un altro Stato membro e per le cure dei pazienti affetti da malattie rare, come previsto dalla direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, che include anche le reti di riferimento europee per le malattie rare, nonché dal regolamento (CE) n. 883/2004 relativo al coordinamento dei sistemi di sicurezza sociale.

Tali servizi di assistenza possono essere forniti da operatori sanitari pubblici o privati e possono essere finanziati da enti pubblici, privati o ibridi, a seconda del sistema sanitario e assistenziale dello Stato membro

(NB: ciò include l'assistenza di persona e la teleassistenza tramite soluzioni di eHealth o mHealth).

Funzioni 2 e 3: uso secondario

Riguardano il riutilizzo dei dati sanitari raccolti inizialmente nel contesto dell'erogazione delle cure, ma che possono essere successivamente riutilizzati per un altro scopo. Questo uso secondario può essere esercitato da enti pubblici, come i sistemi sanitari nazionali, gli enti pubblici di assicurazione sanitaria, gli enti pubblici di ricerca (comprese le università e i laboratori di sanità pubblica), le autorità di regolamentazione, come le agenzie per i medicinali e gli organismi notificati, e l'industria.

Il termine 'industria' include grandi e piccole aziende farmaceutiche e di tecnologia medica, aziende del settore assicurativo e dei servizi finanziari, come valutazione delle norme degli Stati membri dell'UE sui dati sanitari alla luce del GDPR, nonché gli attori dei social media e dell'elettronica di consumo e l'emergente industria dell'intelligenza artificiale.

Le funzioni 2 e 3 possono utilizzare dati che rimangono all'interno di archivi di uso primario, come i sistemi di cartelle cliniche elettroniche, ma possono anche essere riuniti in altri sistemi, come i registri delle malattie che raccolgono dati per calcolare l'incidenza e la prevalenza delle malattie a livello nazionale o regionale

Uso secondario: ulteriore trattamento (GDPR)

La dizione “uso secondario” non è presente nel GDPR, ma deve essere inteso come equivalente alla locuzione “ulteriore trattamento” dei dati come descritto nel principio di limitazione delle finalità di cui all'art. 5, par. 1, lett. b).

Questo principio stabilisce che il trattamento dei dati per una finalità diversa da quella specificata al momento della raccolta non è consentito quando è incompatibile con la finalità iniziale, a meno che tale ulteriore trattamento non abbia (tra l'altro) finalità di ricerca e sia effettuato in conformità alle garanzie descritte nell'art. 89, par. 1, del GDPR.

L'uso dei dati sanitari in conformità alle funzioni 2 e 3 sarà una forma di “ulteriore trattamento” o tali dati possono essere raccolti specificamente per tali funzioni.

La legittimità (base giuridica) dipenderà generalmente dall'esistenza di una legislazione nazionale specifica, come previsto dall'art. 9, lett. h), i) o j); in assenza di tale legislazione, il consenso sarà la legittimazione predefinita per il trattamento dei dati.

European Health Data Space-EHDS: premessa

La disomogeneità di attuazione e interpretazione del GDPR da parte degli Stati membri crea notevoli incertezze giuridiche, che provocano ostacoli all'uso secondario dei dati sanitari elettronici.

Conseguenze:

- le persone fisiche non possono beneficiare di cure innovative
- i responsabili delle politiche non possono reagire in modo efficace a una crisi sanitaria, a causa degli ostacoli che impediscono l'accesso a ricercatori, innovatori, regolatori e responsabili delle politiche ai necessari dati sanitari elettronici.
- a causa delle differenti norme e dell'interoperabilità limitata, i produttori di sanità digitale e i prestatori di servizi di sanità digitale che operano in uno Stato membro incontrano ostacoli e costi aggiuntivi nell'accedere a un altro Stato membro.

Pandemia di COVID-19

La pandemia di COVID-19 ha messo in luce (ancora di più) l'importanza dei dati sanitari elettronici per lo sviluppo di una strategia in risposta alle emergenze sanitarie.

Ha evidenziato l’assoluta necessità di garantire un accesso tempestivo ai dati sanitari elettronici personali non solo per la preparazione e la risposta alle minacce sanitarie e per finalità di cura, ma anche per la ricerca, l'innovazione, la sicurezza dei pazienti, finalità normative, la definizione delle politiche, finalità statistiche o la medicina personalizzata.

Il Consiglio europeo ha riconosciuto l'urgenza di progredire verso la costituzione di uno Spazio europeo dei dati sanitari e di darvi priorità.

European Health Data Space-EHDS

Lo Spazio europeo dei dati sanitari intende:

- promuovere un autentico mercato unico per i sistemi di cartelle cliniche elettroniche

- consentire alle persone di assumere il controllo dei propri dati sanitari e agevolare lo scambio di dati per favorire la prestazione di assistenza sanitaria in tutta l'UE (uso primario dei dati: definito *ex* art. 2, par. 2, lett. d Reg EHDS: trattamento dei dati sanitari elettronici per la fornitura di assistenza sanitaria volta a valutare, mantenere o ripristinare lo stato di salute della persona fisica a cui si riferiscono tali dati, compresa la prescrizione, la distribuzione e la fornitura di medicinali e dispositivi medici, nonché per i pertinenti servizi sociali, amministrativi o di rimborso).

- fornire un sistema coerente, affidabile ed efficiente per il riutilizzo dei dati sanitari in ambiti quali la ricerca, l'innovazione, l'elaborazione delle politiche e le attività normative (uso secondario dei dati: definito *ex* art. 2, par. 2, lett. e Reg. EHDS: trattamento di dati sanitari elettronici per finalità diverse da quelle per cui tali dati erano stati inizialmente raccolti ovvero le finalità relative all'"uso primario").

European Health Data Space-EHDS: Obiettivi

Lo Spazio europeo dei dati sanitari contribuirà alla realizzazione della visione della Commissione per la trasformazione digitale dell'UE entro il 2030, al raggiungimento del triplice obiettivo della **bussola digitale** ha l'obiettivo di utilizzare le capacità tecnologiche per mettere i cittadini e le imprese nelle condizioni necessarie per sfruttare i benefici della trasformazione digitale e di costituire una società più green e in salute.

Bussola Europea per il Digitale 2030

- La **Bussola Europea per il Digitale 2030** ha l'obiettivo di utilizzare le capacità tecnologiche per mettere i cittadini e le imprese nelle condizioni necessarie per sfruttare i benefici della trasformazione digitale e di costituire una società più green e in salute.

I punti cardine per rendere l'Unione Europa digitale sono:

1. **Popolazione dotata di competenze digitali e professionisti altamente qualificati nel settore digitale**
2. **Infrastrutture digitali sostenibili, sicure e performanti**
3. **Trasformazione digitale delle imprese**
4. **Digitalizzazione dei servizi pubblici**

1. Popolazione dotata di competenze digitali e professionisti altamente qualificati nel settore digitale

1. L'Unione Europea mira ad avere cittadini e lavoratori qualificati nel settore digitale grazie a un'istruzione digitale e a politiche con l'obiettivo di attrarre talenti da tutto il mondo.

   La formazione e l'istruzione in campo digitale deve formare cittadini capaci di identificare tentativi di frode, di proteggersi dagli attacchi informatici, e dalle truffe online.

   Entro il 2030:

   1. Dovrebbero essere oltre 20 milioni gli specialisti impiegati nell'UE nel settore delle tecnologie dell'informazione e della comunicazione, con una convergenza tra donne e uomini;
   2. Almeno l'80% della popolazione adulta dovrebbe possedere competenze digitali di base;

2. Infrastrutture digitali sostenibili, sicure e performanti

la connettività, la microelettronica e la capacità di elaborare grandi quantità di dati sono requisiti indispensabili per avere un futuro digitale e per avere un vantaggio competitivo dell'industria.

In questo senso gli obiettivi da raggiungere entro il 2030 sono:

1. tutte le famiglie europee saranno coperte da una rete Gigabit e tutte le zone abitate dalla rete 5G;
2. la produzione di semiconduttori all'avanguardia e sostenibili in Europa, compresi i processori, rappresenterà almeno il 20 % del valore della produzione mondiale;
3. 10.000 nodi periferici a impatto climatico zero e altamente sicuri saranno installati nell'UE e distribuiti in modo da garantire l'accesso a servizi di dati a bassa latenza (pochi millisecondi) ovunque si trovino le imprese;
4. Entro il 2025 l'Europa disporrà del suo primo computer con accelerazione quantistica, che le consentirà di svolgere un ruolo d'avanguardia.

3. Trasformazione digitale delle imprese

Durante la pandemia di COVID-19 per la maggior parte delle imprese è diventato fondamentale utilizzare tecnologie e prodotti digitali. La transizione a una società digitale porta numerosi vantaggi, genera una minore impronta ambientale e comporta una maggiore efficienza energetica e dei materiali. Le PMI sono la maggior parte delle imprese dell'UE, svolgono un ruolo chiave perché sono una sede essenziale di innovazione.

Secondo gli obiettivi Europei entro il 2030:

1. il 75 % delle imprese europee utilizzerà servizi di *cloud computing*, *big da*ta e intelligenza artificiale;
2. oltre il 90 % delle PMI europee raggiungerà almeno un livello di base di intensità digitale;
3. l'Europa aumenterà il numero di *scale-up* innovative e ne migliorerà l'accesso ai finanziamenti, raddoppiando il numero di imprese "unicorno" in Europa.

4. Digitalizzazione dei servizi pubblici

La vita democratica e i servizi pubblici online devono essere garantiti e pienamente accessibili a tutti, incluse le persone con disabilità, e beneficino di un ambiente digitale della migliore qualità che offra servizi e strumenti di facile uso, efficienti e personalizzati con elevati standard in materia sicurezza e tutela della vita privata.

L'obiettivo dell'UE per il 2030 è:

1. Il 100 % dei servizi pubblici principali disponibili online per le imprese e i cittadini europei;
2. Il 100 % dei cittadini europei avrà accesso alle cartelle cliniche (cartelle elettroniche);
3. L'80 % dei cittadini utilizzerà l'identificazione digitale.

European Health Data Space-EHDS

L'EHDS costituisce il pilastro fondamentale di una forte Unione europea della salute ed è il primo spazio comune dei dati in un settore specifico a essere elaborato nel quadro della strategia europea per i dati.
Nella primavera del 2024 il Parlamento europeo e il Consiglio hanno raggiunto un accordo politico sulla proposta della Commissione di uno spazio europeo dei dati sanitari
Per mutuare le parole di Frank Vandenbroucke, Vice Primo Ministro belga e Ministro degli Affari sociali e della Sanità pubblica: «*le nuove norme mirano a consentire a un turista spagnolo di ritirare una ricetta in una farmacia tedesca o ai medici di accedere alle informazioni sanitarie di un paziente belga in cura in Italia*» e che il Regolamento «*consentirà ai pazienti di accedere ai propri dati sanitari ovunque si trovino nell'UE, fornendo al contempo alla ricerca scientifica per importanti motivi di interesse pubblico un patrimonio di dati sicuri che gioveranno notevolmente allo sviluppo di politiche sanitarie*»

Provisional political agreement on a European Health Data Space

- Il 24 aprile 2024 gli eurodeputati hanno votato con 445 favorevoli e 142 contrari (39 astenuti) per approvare l'accordo interistituzionale sulla creazione di uno Spazio europeo per i dati sanitari.
- Questa approvazione si basa sull'accordo, raggiunto lo scorso 14 marzo fra il Parlamento e il Consiglio dell'Unione europea, in relazione alla proposta di Regolamento presentata dalla Commissione il 3 maggio 2022.
- Il Regolamento consentirà ai pazienti di accedere ai propri dati sanitari in formato elettronico, anche da uno Stato membro diverso da quello in cui vivono, e consentirà agli operatori sanitari di consultare le cartelle cliniche dei loro pazienti con il loro consenso (uso primario), anche da altri Paesi dell'UE. Queste cartelle cliniche elettroniche (EHR) includerebbero i resoconti dei pazienti, le prescrizioni elettroniche, le immagini mediche e i risultati di laboratorio.
- Il Regolamento consentirà di trasferire i dati sanitari in modo sicuro agli operatori sanitari di altri Paesi dell'UE (sulla base dell'infrastruttura MyHealth@EU), ad es. quando i cittadini si trasferiscono in un altro Stato. Sarà possibile scaricare gratuitamente la cartella clinica.

La strategia europea per i dati

Il Regolamento sullo Spazio Europeo dei Dati Sanitari si basa sugli artt. 16 e 114 del Trattato sul funzionamento dell'Unione Europea e rappresenta uno dei pilastri dell'ambiziosa "Strategia Europea per i Dati" della Commissione, che include una serie di atti normativi paralleli, come il Data Act e il Data Governance Act. Partendo dal presupposto che i dati rappresentano una risorsa essenziale per la crescita economica, la competitività, l'innovazione, la creazione di posti di lavoro e il progresso sociale in generale, la "Strategia Europea per i Dati" ha l'obiettivo di creare un "mercato unico dei dati", che garantisca la competitività globale dell'Europa e la sovranità sui dati, anche attraverso la creazione di spazi comuni per la condivisione delle informazioni.

Basi giuridiche

Lo Spazio europeo dei dati sanitari si fonda, tra l'altro, sui testi seguenti:

- regolamento generale sulla protezione dei dati (GDPR)
- regolamento sulla governance dei dati
- regolamento sui dati
- direttiva sulla sicurezza delle reti e dei sistemi informatici

Essendo trasversali, questi testi prevedono norme che si applicano anche al settore sanitario. Tuttavia, lo Spazio europeo dei dati sanitari fornirà norme settoriali specifiche, considerata la sensibilità dei dati relativi alla salute.

Lo Spazio europeo dei dati sanitari prevede anche deroghe per:

- l'uso primario, consentendo agli Stati membri di offrire una deroga totale per le infrastrutture da costruire nell'ambito dello spazio
- l'uso secondario, in modo da permettere un buon equilibrio tra il rispetto dei desideri dei pazienti e la possibilità di garantire che i dati giusti siano a disposizione delle persone giuste nell'interesse pubblico.

Contenuto del Regolamento

L'art. 1, paragrafo 1, del testo indica che il Regolamento istituisce lo Spazio Europeo dei Dati Sanitari individuando regole, standard e infrastrutture comuni nonché un quadro per la governance dei dati sanitari, con l'obiettivo di facilitare l'accesso ai dati sanitari elettronici ai fini del loro utilizzo primario e secondario.

In particolare, il Regolamento:

1. specifica e integra i diritti previsti dal GDPR in relazione all'uso primario e secondario dei dati sanitari elettronici;
2. stabilisce regole comuni sugli *electronic health record systems* (EHR systems), con particolare riferimento a due componenti software obbligatorie che dovranno essere adottate per garantire la possibile condivisione dei dati al di là dei confini dei singoli Stati membri.

   Tali componenti sono *l'European interoperability component for EHR systems* e l'*European logging component for EHR systems* (introdotte nel testo dal Parlamento). Le medesime regole varranno anche per le applicazioni per il wellness rispetto a cui i produttori intendano stabilire l'interoperabilità con gli *EHR systems* per l'uso primario dei dati;
3. istituisce un'infrastruttura transnazionale per consentire l'uso primario e secondario dei dati sanitari elettronici all'interno dell'Unione europea;
4. prevede norme per la governance e il coordinamento a livello nazionale ed europeo per l'uso primario e secondario dei dati sanitari elettronici.

Electronic health record systems

- **Obbligo di conformità degli EHR *systems* alle specifiche previste per il formato europeo di scambio dei dati sanitari elettronici**, in modo da garantire la **sicurezza** dei dati e renderne possibile la **condivisione** al di là dei confini degli Stati membri. Attualmente, tale possibilità incontra ostacoli significativi, derivanti dal diverso livello di digitalizzazione dei dati sanitari nei Paesi dell'Unione.
- Per *electronic health record system* s'intende qualunque dispositivo o software utilizzato per l'elaborazione di *electronic health record*, ossia qualunque insieme di dati sanitari elettronici raccolti nel sistema sanitario, relativi a una persona fisica e utilizzati per scopi sanitari: il Regolamento, oltre a prevedere specifici obblighi in capo a importatori e distributori degli "*EHR systems*", stabilisce una serie di requisiti per i produttori di *EHR systems*, che dovranno predisporre e aggiornare la documentazione tecnica prevista dalla normativa, le schede informative e le dichiarazioni di conformità nonché applicare ai sistemi la marcatura CE. Inoltre è previsto **un ambiente digitale europeo di *testing* (*European digital testing environment*), che la Commissione dovrà sviluppare per la valutazione dei componenti degli *EHR systems***, rendendo anche disponibile il relativo software in formato *open source*.
- Anche gli Stati membri sono tenuti a istituire un ambiente digitale di *testing* per la medesima finalità di valutazione dei componenti degli *EHR systems*, in conformità con le specifiche previste dalla Commissione con successivi atti esecutivi del Regolamento. Prima di immettere sul mercato gli *EHR systems*, i produttori saranno tenuti a utilizzare gli ambienti di *testing* per valutare i propri sistemi e i risultati dei test dovranno essere inclusi all'interno della documentazione tecnica che accompagna i sistemi stessi.
- Infine, i produttori di applicazioni per il *wellness* potranno stabilire l'interoperabilità di tali applicazioni con gli *EHR systems* per l'uso primario dei dati, informando debitamente gli utenti anche in relazione agli effetti di tale interoperabilità. Ad ogni modo, la condivisione o la trasmissione dei dati tramite tali applicazioni sarà possibile solo con il previo consenso dell'utente, che dovrà essere messo in condizione di scegliere quali categorie di dati sanitari disponibili sull'applicazione desidera inserire negli *EHR systems*.

Uso primario dei dati sanitari elettronici

L'art. 5 individua le categorie di dati sanitari elettronici che dovranno essere resi accessibili e condivisi per finalità di cura e assistenza del paziente (*i.e.* per uso primario), lasciando agli Stati membri la possibilità di aggiungere ulteriori categorie di informazioni. Tali categorie – definite *priority categories of personal electronic health data for primary use* e meglio specificate nell'Allegato 1 del Regolamento – includono:

- informazioni generali sul paziente: ad es. dati identificativi e di contatto, informazioni su eventuali coperture assicurative del paziente, le sue vaccinazioni, allergie, gravidanze, i farmaci assunti o in corso di assunzione, piano di cura, storia clinica del paziente;
- informazioni su prescrizioni elettroniche;
- informazioni su dispensazioni elettroniche;
- immagini mediche e relativi referti;
- risultati di analisi mediche, incluse le analisi di laboratorio e altri esami diagnostici con i relativi referti;
- rapporti di dimissione del paziente.

La Commissione europea avrà il compito di chiarire, con appositi atti di esecuzione, il formato di scambio delle suddette informazioni, che dovrà in ogni caso essere di uso comune, leggibili da dispositivo automatico e consentire la trasmissione di dati sanitari elettronici tra diversi dispositivi, applicazioni e operatori sanitari, supportando sia la trasmissione di dati sanitari strutturati che di dati non strutturati. Gli Stati membri dovranno assicurare che i dati sanitari elettronici sopra elencati siano rilasciati nel formato di scambio previsto dalla Commissione europea.

Uso primario dei dati sanitari elettronici e diritti dei pazienti

- Il Regolamento prevede diversi articoli che disciplinano in modo dettagliato le modalità di esercizio di una serie di diritti da parte dei pazienti e dei loro rappresentanti, fra cui il diritto di accesso ai dati sanitari elettronici, il diritto di integrare tali dati direttamente tramite il proprio "*electronic health record*" (rendendo però le informazioni aggiunte chiaramente distinguibili da quelle inserite dai professionisti sanitari), il diritto di rettifica dei dati sanitari.
- In tale contesto, la novità più significativa è rappresentata dalla possibilità che gli Stati membri prevedano il c.d. diritto di *opt-out*, vale a dire il diritto dei pazienti a inibire l'accesso ai propri dati sanitari sia da parte degli operatori sanitari, per l'uso primario, che da parte degli altri soggetti legittimati ad utilizzare i dati per l'uso secondario, sebbene in tal caso il diritto di *opt-out* sia soggetto a una serie di condizioni rigorose.
- Le scelte compiute dai pazienti devono comunque essere reversibili, in modo da permettere a questi ultimi di modificarle qualora lo ritengano opportuno.
- Un'ulteriore importante novità, inserita nell'ultima versione del Regolamento, è rappresentata dal divieto, per gli operatori sanitari, di addebitare dei costi:
  - ai pazienti, per aver chiesto l'accesso ai propri dati sanitari o per averli condivisi; e
  - ad altri soggetti, per aver reso loro disponibili i dati sanitari elettronici.

Uso secondario dei dati consentito

Il Regolamento mira anche ad agevolare l'accesso ai dati sanitari elettronici per finalità ulteriori rispetto a quelle di cura e assistenza dei pazienti, vale a dire per l'uso secondario dei dati. In particolare, il Regolamento individua una serie di finalità per le quali è consentito l'uso secondario e altre per cui deve considerarsi radicalmente vietato.

Rientrano fra le finalità il cui perseguimento è consentito dal Regolamento quelle di:

- pubblico interesse nel campo della salute pubblica e del lavoro, come le attività per proteggere la salute da gravi minacce transnazionali, le attività di monitoraggio della salute pubblica o le attività volte ad assicurare alti livelli di qualità e sicurezza dell'assistenza sanitaria, inclusa la sicurezza dei pazienti, dei medicinali e dei dispositivi medici;
- *policy making* e svolgimento di attività regolatorie per supportare organi della pubblica amministrazione e istituzioni europee nell'esecuzione dei propri compiti, nel settore sanitario;
- statistica, legate al settore sanitario o dell'assistenza;
- formazione nel settore sanitario o dell'assistenza, a livello di istruzione professionale o superiore;
- ricerca scientifica relativa al settore sanitario o dell'assistenza, che sia di beneficio per pazienti, professionisti sanitari e amministratori della sanità;
- miglioramento dell'erogazione delle cure, l'ottimizzazione dei trattamenti e la fornitura di assistenza sanitaria.

Uso secondario dei dati vietato

L'utilizzo dei dati sanitari elettronici non sarà consentito per le seguenti finalità:

- assumere decisioni che possano avere effetti sociali, economici o legali negativi sull'individuo o su un gruppo di individui;
- assumere decisioni sull'individuo o su un gruppo di individui in relazione a offerte di lavoro o offerte di beni e servizi (ad es. rifiutando di concedere una copertura assicurativa o un prestito);
- attività di marketing;
- sviluppo di prodotti o servizi che possano danneggiare gli individui, la salute pubblica o la società in generale, ad es. sostanze stupefacenti, alcolici, prodotti da tabacco o nicotina, ecc.;
- altre attività in conflitto con la morale (*ethical provisions*), secondo le previsioni della normativa degli Stati membri.

L'art. 33 del Regolamento individua poi le categorie minime di dati che devono essere resi disponibili per l'uso secondario (*minimum categories of electronic data for secondary use*), con un elenco ben più corposo rispetto a quello riportato all'art. 5 per l'utilizzo primario dei dati sanitari. Gli Stati Membri potranno anche prevedere ulteriori categorie di informazioni da rendere accessibili per l'uso secondario.

Uso secondario dei dati vietato

Gli Stati membri potranno inoltre adottare misure più severe per disciplinare l'accesso a determinati tipi di dati sensibili (ad esempio, quelli genetici), per scopi di ricerca scientifica, prevedendo ulteriori limitazioni rispetto a quelle stabilite dal Regolamento.

Nel Regolamento sono stati inoltre individuati gli attori principali in relazione all'uso secondario dei dati sanitari, con i relativi compiti:

- gli organismi per l'accesso ai dati sanitari (*health data access bodies*), designati dagli Stati membri al fine principale di autorizzare l'accesso ai dati a seguito della ricezione di una richiesta di accesso per uso secondario;
- i titolari di dati sanitari (*health data holders*), vale a dire qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro organismo del settore sanitario o assistenziale che abbia
  - (i) il diritto o l'obbligo di trattare i dati sanitari elettronici in qualità di titolare o contitolare del trattamento, ai sensi del GDPR; oppure
  - (ii) la capacità di mettere a disposizione, anche per registrare, fornire, limitare l'accesso o scambiare dati sanitari elettronici non personali, attraverso il controllo della progettazione tecnica di un prodotto e dei servizi correlati.
- gli utenti di dati sanitari (*health data users*), ovvero le persone fisiche o giuridiche, comprese le istituzioni, gli organismi o le agenzie dell'UE, a cui è stato legittimamente concesso l'accesso ai dati sanitari elettronici per uso secondario.

Va sottolineata l'esenzione rispetto agli obblighi disposti in relazione all'uso secondario dei dati sanitari elettronici per singoli ricercatori e persone fisiche e persone giuridiche che si qualificano come microimprese.

Uso secondario e diritto di *opt-out* dei pazienti

Anche in relazione all'uso secondario viene garantito ai pazienti il diritto di *opt-out*.

Tuttavia resta consentito l'accesso per scopi

- di interesse pubblico,
- di sviluppo di politiche sanitarie
- per finalità statistiche e di ricerca condotte nel pubblico interesse.

Viene inoltre prevista la figura del titolare di dati sanitari di fiducia (*trusted data holder*), al fine di snellire le procedure per autorizzare l'accesso ai dati per fini secondari. In particolare, si prevede che le richieste per l'accesso ai dati detenuti dal *trusted data holder* possa essere inoltrata a tale soggetto da parte dell'organismo per l'accesso ai dati sanitari ai fini di delegare al *trusted data holder* la decisione in merito alle richieste di accesso per fini secondari. Spetterà agli Sati membri individuare, alla luce dei criteri fissati dal Regolamento, la procedura per richiedere lo status *trusted data holder* da parte dei titolari dei dati interessati.

Considerazioni sul Regolamento - *European Health Data Space*

PRO

- L'EHDS dovrebbe favorire il potenziale di ricerca dei dati sanitari in formato anonimo o pseudonimizzato. I dati, tra cui cartelle cliniche, sperimentazioni cliniche, agenti patogeni, indicazioni sanitarie e rimborsi, dati genetici, informazioni sui registri sanitari pubblici, dati sul benessere e informazioni su risorse, spese e finanziamenti sanitari, potrebbero essere trattati per scopi di interesse pubblico, tra cui ricerca, statistica e politica (uso secondario).
- I dati potrebbero, per esempio, essere utilizzati per trovare trattamenti per le malattie rare, dove i piccoli set di dati e la frammentazione attualmente impediscono progressi nelle cure.
- NB: L'uso secondario non sarà consentito per scopi commerciali, inclusa la pubblicità, la valutazione di richieste assicurative o condizioni di prestito o l'assunzione di decisioni sul mercato del lavoro. Le decisioni in materia di accesso saranno prese dagli organismi nazionali di accesso ai dati.

CONTRO

- una serie di rischi notevoli per i pazienti e la società tutta, in particolare il rischio di accesso abusivo ai dati sanitari elettronici
  - per la privacy degli individui,
  - per la tutela dei pazienti
  - per la protezione dei segreti commerciali degli operatori del settore.
- Altri gravi rischi possono derivare dall'utilizzo di dati imprecisi, incompleti o non aggiornati o dalla loro eventuale perdita: basti pensare che tali eventi potrebbero determinare il personale sanitario a compiere scelte scorrette sui trattamenti da somministrare ai pazienti, con un impatto negativo sulla loro salute.
- Altri rischi riguardano il possibile utilizzo dei dati per finalità non coerenti con quelle previste dal Regolamento e gli effetti discriminatori che questo potrebbe generare per gli interessati

Prossimi passi

Il Regolamento deve ancora essere approvato formalmente dal Consiglio.

Una volta pubblicato sulla Gazzetta Ufficiale dell'UE (presumibilmente nell'autunno del 2024), entrerà in vigore venti giorni dopo.

Verrà applicato due anni dopo, con alcune eccezioni, compreso l'uso primario e secondario delle categorie di dati, che si applicherà da quattro a sei anni dopo, a seconda della categoria.