RICERCA SCIENTIFICA E TRATTAMENTO DEI DATI SANITARI (ANCHE) ATTRAVERSO L'INTELLIGENZA ARTIFICIALE

Il problema giuridico

Bilanciamento fra:

- Ricerca scientifica e
- La tutela della persona rispetto alla circolazione dei propri dati

«*l'innovazione tecnologica porta[no] la persona in un mercato in espansione: quello dei dati. L'autodeterminazione informativa è così chiamata, ora attraverso le disposizioni del GDPR, a trovare declinazioni che rispondano ad esigenze nuove dell'economia, pur continuando a difendere la personalità dell'individuo*». (S. CORSO, *Autodeterminazione e dati sanitari*, Torino, 2025, p. 127)

Le fonti normative di riferimento

Livello Europeo

1. **Regolamento UE 2016/679 (GDPR)** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
2. **Regolamento UE 2024/1689** (c.d. «***AI Act***») ha l'obiettivo di dettare un insieme armonizzato di regole in materia di intelligenza artificiale
3. **Regolamento UE 2025/327** relativo allo spazio europeo dei dati sanitari, con l'obiettivo di favorire la sicurezza nello scambio di dati sanitari (anche) ai fini di ricerca

Livello Nazionale

1. **D.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali)**
2. **D.lgs. 10 agosto 2018, n. 101 (adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679)**
3. **Decreto 7 settembre 2023 (Fascicolo sanitario elettronico 2.0.)**
4. **Decreto Interministeriale 31 dicembre 2024 – Ministero della Salute (EDS - Ecosistema dei Dati Sanitari)**
5. **L. 23 settembre 2025, n. 132**
   - Contiene «*princìpi in materia di ricerca, sperimentazione, sviluppo, adozione e applicazione di sistemi e di modelli di intelligenza artificiale. Promuove un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità. Garantisce la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali dell'intelligenza artificiale*». (Art. 1)

Le Basi Giuridiche – Art. 6 del GDPR (Liceità del trattamento)

«*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»

Le Basi Giuridiche – Art. 9 del GDPR (categorie particolari di dati personali)

• **Dati sanitari** («**dati relativi alla salute**»): «*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. 1, comma 15, GDPR)

•I **dati sanitari** sono compresi fra le «***categorie particolari di dati***» (Art. 9 GDPR):

«*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, comma 1, GDPR)

Le Basi Giuridiche – Art. 9 del GDPR (categorie particolari di dati personali)

«*Il paragrafo 1 non si applica se si verifica uno dei seguenti casi*» (Art. 9, comma 2, GDPR):

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 paragrafo 1*»

- **consenso dell'interessato**: «*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*» (Art. 4, comma 11, GDPR)

b) **Interesse pubblico rilevante:** previsto dal diritto dell'Unione o degli Stati membri (Art. 9, comma 2, lett. g, GDPR)

c) **Interesse pubblico** nel settore della **sanità pubblica** (Art. 9, comma 2, lett. i, GDPR)

d) **Ricerca scientifica:** (Art. 9.2, lett. j, GDPR) con misure tecniche e organizzative appropriate (es. pseudonimizzazione)

Le Basi Giuridiche – Art. 89 del GDPR (Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici)

1. Il **trattamento** a fini di archiviazione nel pubblico interesse, di **ricerca scientifica** o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del **principio della minimizzazione dei dati**. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

2. Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere **deroghe** ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

3. Se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

4. Qualora il trattamento di cui ai paragrafi 2 e 3 funga allo stesso tempo a un altro scopo, le deroghe si applicano solo al trattamento per le finalità di cui ai medesimi paragrafi.

La Modifica dell'Art. 110 del Codice Privacy

Il **consenso dell'interessato** per il trattamento dei **dati relativi alla salute**, a **fini** di **ricerca scientifica in campo medico**, **biomedico** o **epidemiologico**, **non** è **necessario** quando la ricerca è effettuata:

a) in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), GDPR
   - incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del GDPR

b) a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure

c) rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca

In questi casi:

- il **titolare del trattamento** adotta **misure** appropriate per **tutelare** i diritti, le libertà e i legittimi interessi dell'**interessato**, il programma di ricerca è oggetto di **motivato parere favorevole** del competente **comitato etico** a livello territoriale

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale

1. **Basi giuridiche del trattamento**
   a. diritto dell'Unione o degli Stati membri
   b. proporzionalità rispetto alla finalità perseguita
   c. rispetto del diritto alla protezione dei dati
   d. previsione di misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9, par. 2, lett. g) del GDPR; cfr. sul punto sentenza della Corte Costituzionale n. 20 del 2019; considerando 71 e art. 22, par. 4, del GDPR)
2. **I principi di accountability e di privacy by design e by default**
   a. *privacy by design* e *by default* (riservatezza/protezione dei dati fin dalla progettazione e per impostazione – art. 25, par. 1, GDPR): nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario devono essere adottate misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (art. 5 GDPR) e integrate nel trattamento le garanzie necessarie per soddisfare i requisiti del GDPR e tutelare i diritti e le libertà degli interessati
      - sin dalla sua costruzione l'ambiente digitale va pensato come un insieme di strutture che garantiscano il diritto alla protezione dei dati personali e l'architettura dello spazio elettronico deve rispondere a questa logica
   b. *accountability* (responsabilizzazione dei soggetti che operano il trattamento dei dati): quando la legittimazione del trattamento riposa sul consenso dell'interessato, il titolare deve essere in grado di dimostrare che questi lo abbia prestato (art. 5, par. 2, GDPR)
   c. proporzionalità del trattamento rispetto all'interesse pubblico perseguito, ponendosi l'obiettivo di ottenere un reale effetto di tutela

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale

3. **Ruoli**
   a) **Titolare** (**N.B.**: necessario che vi sia una idonea base giuridica che conferisca a tale soggetto il compito di svolgere il trattamento; non sufficiente un mero presupposto fattuale)→ il soggetto sul quale ricadono:
      i. le decisioni di fondo relativamente alle finalità e ai mezzi del trattamento dei dati personali
      ii. la responsabilità generale (cd. "***accountability***") sui trattamenti posti in essere dallo stesso o da altri "per [suo] conto", in qualità di responsabili ai sensi dell'art. 28 GDPR
   b) **Responsabile** → svolgimento di attività delegate dal titolare il quale, all'esito di proprie scelte organizzative, può individuare uno o più soggetti particolarmente qualificati al loro svolgimento (conoscenze specialistiche, affidabilità, risorse e sicurezza del trattamento)

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale

4. **Tre principi cardine** (per l'utilizzo di algoritmi e di strumenti di IA nell'esecuzione di compiti di rilevante interesse pubblico):
   - **a)** **principio di conoscibilità:** l'interessato ha il diritto di conoscere l'esistenza di processi decisionali basati su trattamenti automatizzati e, in tal caso, di ricevere informazioni significative sulla logica utilizzata, sì da poterla comprendere;
   - **b)** **principio di non esclusività della decisione algoritmica**: deve comunque esistere nel processo decisionale un intervento umano capace di controllare, validare ovvero smentire la decisione automatica (c.d. «*human in the loop*»);
   - **c)** **principio di non discriminazione algoritmica:** è opportuno che il titolare del trattamento utilizzi sistemi di IA affidabili che riducano le opacità, gli errori dovuti a cause tecnologiche e/o umane, verificandone periodicamente l'efficacia anche alla luce della rapida evoluzione delle tecnologie impiegate, delle procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate
     - i. garantire, che siano rettificati i fattori che comportano inesattezze dei dati e
     - ii. minimizzare il rischio di errori, visti i potenziali effetti discriminatori che un trattamento inesatto di dati sullo stato di salute può determinare nei confronti di persone fisiche

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale

5. **Valutazione d'impatto sulla protezione dei dati (VIP)** → obbligo per i titolari di:
   a) 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 GDPR)
   b) 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 GDPR)

- **sistema centralizzato** a livello nazionale → per realizzare servizi sanitari con strumenti di IA, determinando un trattamento sistematico, su larga scala, di particolari categorie di dati personali (art. 9 GDPR) di soggetti vulnerabili, attraverso l'uso di nuove tecnologie e presentando un rischio elevato per i diritti e le libertà degli interessati:
- **Trattamenti «a rischio elevato»**→ richiedono preventivamente una valutazione di impatto:
  1. individuazione delle misure idonee a tutelare i diritti e le libertà fondamentali degli interessati
  2. garantire il rispetto dei principi generali del GDPR
  3. consentire l'analisi della proporzionalità dei trattamenti effettuati
- **Valutazione d'impatto**: rischi propri di una banca dati contenente le informazioni sanitarie di tutta la popolazione assistita sul territorio nazionale: i) perdita dei requisiti di qualità dei dati (es. mancato o errato allineamento e aggiornamento); ii) revoca del consenso, se costituisce la base giuridica del trattamento originario; iii) re-identificazione dell'interessato in considerazione delle possibili interconnessioni con molteplici sistemi informativi e banche dati e all'utilizzo dei dati per finalità non compatibili

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale

6. **Qualità dei dati** Il titolare del trattamento deve garantire che i dati siano esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati non corretti rispetto alle finalità per le quali sono trattati (**principio di «esattezza» -** art. 5, par. 1, lett. d), GDPR).
   - ❖ **N.B.**: Il dato non aggiornato o inesatto influenzerebbe inoltre anche l'efficacia e la correttezza dei servizi che i suddetti sistemi di IA, che si basano infatti sulla rielaborazione di tali dati, intendono realizzare.
7. **Integrità e riservatezza**

i dati personali devono essere «*trattati in maniera da garantire un'adeguata sicurezza (…), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)*» (art. 5, par. 1, lett. f), GDPR)

- ➢ la base giuridica del trattamento dei dati effettuati attraverso sistemi nazionali di IA deve indicare misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato, comprese misure adeguate a mitigare i rischi correlati all'uso di tecniche di IA su dati sanitari, trattati su larga scala, di soggetti vulnerabili che possono portare all'adozione di decisioni automatizzate.

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale

8. Correttezza e trasparenza

trasparenza e correttezza nei processi decisionali fondati su trattamenti automatizzati (sistemi di IA) → evitare rischi discriminatori derivati dall'uso di tali strumenti

- **consapevolezza** nelle collettività di riferimento (i.e. la totalità degli assistiti del Sistema Sanitario Nazionale) in relazione all'impiego dei sistemi di intelligenza artificiale e comprensione in relazione al loro funzionamento
- **partecipazione dei differenti *stakeholder*** in relazione al ciclo di vita dei sistemi di intelligenza artificiale per uno sviluppo sostenibile e una governance rispettosa dei diritti degli interessati

Misure e adempimenti da implementare nella predisposizione dei sistemi di IA in sanità:

1. assicurare che la **base giuridica** del **trattamento** sia chiara, prevedibile e resa conoscibile agli interessati anche attraverso specifiche campagne di informazione
2. consultare gli *stakeholder* e gli interessati nell'ambito dello svolgimento della valutazione d'impatto (art. 35, par. 9, GDPR);
3. pubblicare, anche solo per estratto, la valutazione d'impatto;
4. predisporre le informazioni da rendere agli interessati, con gli elementi di cui agli artt. 13 e 14 GDPR in termini chiari, concisi e comprensibili;
5. informare non solo in merito agli elementi di cui ai richiamati artt. 13 e 14 GDPR, ma anche evidenziando:
   I. se il trattamento sia effettuato nella fase di apprendimento dell'algoritmo (sperimentazione e validazione) ovvero nella successiva fase di applicazione dello stesso, nell'ambito dei servizi sanitari, rappresentando le logiche e le caratteristiche di elaborazione dei dati;
   II. se sussistono eventuali obblighi e responsabilità dei professionisti sanitari, a cui si rivolge l'interessato, ad utilizzare servizi sanitari basati sull'IA;
   III. i vantaggi, in termini diagnostici e terapeutici, derivanti dall'utilizzo di tali nuove tecnologie;
6. assicurare modalità efficaci di esercizio dei diritti degli interessati previsti dal GDPR e dalle specifiche discipline di settore, tenuto anche conto dei diversi ruoli rivestiti dai soggetti coinvolti nel trattamento;
7. nel caso di perseguimento di finalità di cura, garantire che i servizi di elaborazione dei dati basati su sistemi di IA, siano realizzati solo a seguito di una espressa richiesta di attivazione del professionista sanitario e non in modo automatico;
8. regolamentare i profili di responsabilità professionale connessi alla scelta del professionista sanitario di affidarsi o meno ai servizi di elaborazione dei dati sanitari dei propri pazienti effettuati sulla base di sistemi di IA.

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale

9. Supervisione umana

- Ci sono limiti se le decisioni vengono prese solo sulla base di dati elaborati mediante sistemi di Intelligenza artificiale → necessario un effettivo coinvolgimento degli esseri umani:
  1. supervisione altamente qualificata
  2. liceità del trattamento
     - ✓ assicurare il rispetto del diritto di non essere assoggettato a una decisione basata esclusivamente su un trattamento automatizzato → rischio di imprecisione:
       - In fase di *addestramento* degli algoritmi, la predizione del rischio di sviluppare malattie proporzionale al numero, alla qualità e all'accuratezza dei dati inseriti e alle esperienze immagazzinate su un determinato tema

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale

10. Ulteriori profili.

- Atteggiamento eticamente corretto, sicuro e trasparente della tecnologia dell'intelligenza artificiale → opportuno preferire fornitori che sin da subito:
  a) si preoccupano di svolgere una valutazione di impatto sulla protezione dei dati prima della commercializzazione dei propri prodotti (e fermo l'obbligo in capo al titolare del trattamento di svolgerne una specifica);
  b) abbiano eventualmente anche condotto una specifica valutazione di impatto per l'IA, sicura, trasparente e affidabile.

Regolamento UE 2025/327 – Spazio europeo dei dati sanitari

• **uso primario** (per la prestazione di assistenza sanitaria)→ i pazienti avranno il diritto di limitare l'accesso degli operatori sanitari all'insieme o a parte dei loro dati sanitari scambiati attraverso le infrastrutture dello Spazio europeo dei dati sanitari.

- Gli Stati membri possono offrire l'opzione di non partecipare allo scambio transnazionale di dati sanitari elettronici nell'ambito dello spazio europeo dei dati sanitari. **MA** i dati dei pazienti saranno comunque conservati ed elaborati digitalmente all'interno dell'infrastruttura sanitaria del paese.

• **uso secondario** (finalità diverse da quelle iniziali per le quali tali dati sono stati raccolti o prodotti) → possibile unicamente per le finalità specifiche previste dal regolamento, sulla base di un'autorizzazione rilasciata da un organismo responsabile dell'accesso ai dati sanitari → Art. 53, lett. e): «***ricerca scientifica nel settore sanitario*** *o dell'assistenza che contribuisce alla sanità pubblica o alla valutazione delle tecnologie sanitarie o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di favorire gli utenti finali, quali i pazienti, i professionisti sanitari e gli amministratori sanitari, tra cui: i) attività di sviluppo e innovazione per prodotti o servizi; ii) attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di IA e applicazioni di sanità digitale*»

- **diritto di opporsi all'uso secondario dei dati** (Art. 71). **MA**, nel rispetto di rigorose garanzie, compresi i requisiti di trasparenza, i dati di chi si oppone potrebbero comunque essere utilizzati per alcuni importanti scopi di interesse pubblico.

Regolamento UE 2024/1689 – Regole armonizzate sull'intelligenza artificiale

• **considerando 47**: «*I sistemi di IA potrebbero avere un impatto negativo sulla salute e sulla sicurezza delle persone, in particolare quando tali sistemi sono impiegati come componenti di sicurezza dei prodotti. Coerentemente con gli obiettivi della normativa di armonizzazione dell'Unione di agevolare la libera circolazione dei prodotti nel mercato interno e di garantire che solo prodotti sicuri e comunque conformi possano essere immessi sul mercato, è importante che i rischi per la sicurezza che un prodotto nel suo insieme può generare a causa dei suoi componenti digitali, compresi i sistemi di IA, siano debitamente prevenuti e attenuati. Ad esempio, i robot sempre più autonomi, sia nel contesto della produzione sia in quello della cura e dell'assistenza alle persone, dovrebbero essere in misura di operare e svolgere le loro funzioni in condizioni di sicurezza in ambienti complessi. Analogamente,* ***nel settore sanitario****, in cui la posta in gioco per la vita e la salute è particolarmente elevata, è opportuno che i* ***sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati***».

Decreto Interministeriale 31 dicembre 2024 (EDS – Ecosistema dei Dati Sanitari)

Art. 17

- È possibile l'utilizzo di appositi servizi di estrazione dei dati anonimizzati per finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico
- I soggetti pubblici e privati che istituzionalmente perseguono finalità di studio e di ricerca scientifica in campo medico, biomedico ed epidemiologico presentano ad Agenzia nazionale per i servizi sanitari regionali (Agenas) una richiesta di estrazione di dati anonimizzati, corredata da un relativo progetto di ricerca redatto conformemente alle regole metodologiche e etiche, e se del caso alle regole deontologiche per trattamenti a fini statistici e di ricerca scientifica
- L'Agenas, in qualità di responsabile del trattamento, valuta le richieste di cui al periodo precedente, le finalità perseguite dal soggetto richiedente, e accede al servizio di estrazione dei dati al fine di evadere le richieste e fornire i dati anonimizzati.
- I dati anonimizzati resi disponibili attraverso i servizi di estrazione in oggetto non sono conservati nell'EDS.

Decreto 7 settembre 2023
(Fascicolo sanitario elettronico 2.0.)

- art. 9 (**diritti dell'interessato**) riconferma il **diritto** all'**oscuramento**:
  - Il suo esercizio comporta che i documenti scelti dall'assistito stesso – e quelli logicamente connessi – non siano più visibili nel Fascicolo sanitario elettronico, compreso lo stesso oscuramento (c.d. «oscuramento dell'oscuramento»)
  - L'oscuramento **non** è **irreversibile** e può essere revocato
  - **N.B.**: il documento oscurato non viene rimosso dal Fascicolo sanitario elettronico.
    - La facoltà di cancellare o rimuovere dati o documenti caricati nel Fascicolo sanitario elettronico non è prevista, a prescindere dal loro contenuto effettivo e dalla sensibilità della relativa informazione.