UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unIMC

DIGITAL HEALTH EVOLUTION : FSE and DATA ECOSYSTEM (EDS)

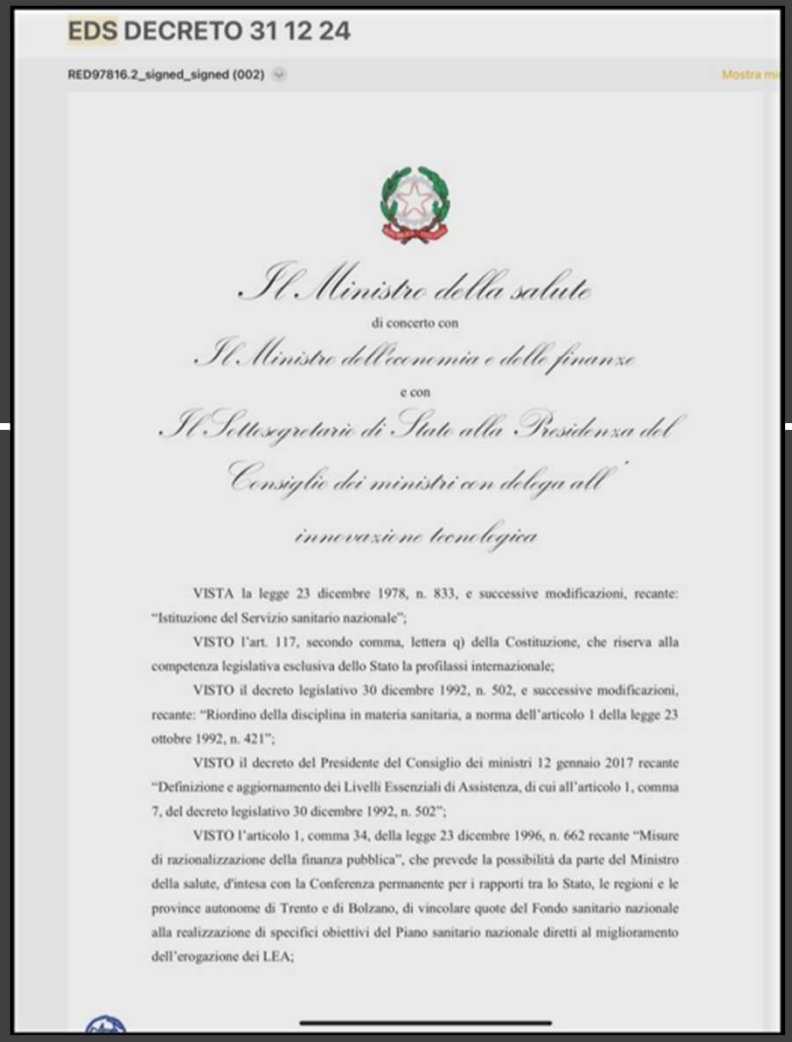
Dott.ssa Angelica Iaia
Socio Apihm Associazione Privacy and Information Heathcare Manager
Polo Ospedaliero Scientifico Medea Brindisi

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

31. 12 2024: il Governo approva il decreto dell’EDS, l’Ecosistema Dati Sanitari.

Un fatto storico: cambia il medium per la sanità italiana

Il provvedimento era fermo dall’agosto 2022


EDS DECRETO 31 12 24

RED97816.2_signed_signed (002)

Il Ministro della salute

di concerto con

Il Ministro dell'economia e delle finanze

e con

Il Sottosegretario di Stato alla Presidenza del Consiglio dei ministri con delega all'innovazione tecnologica

VISTA la legge 23 dicembre 1978, n. 833, e successive modificazioni, recante: "Istituzione del Servizio sanitario nazionale";

VISTO l'art. 117, secondo comma, lettera q) della Costituzione, che riserva alla competenza legislativa esclusiva dello Stato la profilassi internazionale;

VISTO il decreto legislativo 30 dicembre 1992, n. 502, e successive modificazioni, recante: "Riordino della disciplina in materia sanitaria, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421";

VISTO il decreto del Presidente del Consiglio dei ministri 12 gennaio 2017 recante "Definizione e aggiornamento dei Livelli Essenziali di Assistenza, di cui all'articolo 1, comma 7, del decreto legislativo 30 dicembre 1992, n. 502";

VISTO l'articolo 1, comma 34, della legge 23 dicembre 1996, n. 662 recante "Misure di razionalizzazione della finanza pubblica", che prevede la possibilità da parte del Ministro della salute, d'intesa con la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, di vincolare quote del Fondo sanitario nazionale alla realizzazione di specifici obiettivi del Piano sanitario nazionale diretti al miglioramento dell'erogazione dei LEA;

Il 15 luglio 2022 il Garante per la Protezione dei Dati Personali ha espresso un parere non positivo sullo schema di decreto relativo all'**Ecosistema Dati Sanitari (EDS)** presentato dal Ministero della Salute

Ecosystem of Health Data: Garante's Critical Review

- adottato il 22 agosto 2022, il parere sottolinea la presenza di "carenze strutturali e sostanziali" che rendono il testo non coerente con il quadro normativo e in violazione della disciplina sulla protezione dei dati personali, richiedendo una profonda revisione.

- Il suo scopo è **garantire il coordinamento informatico e assicurare servizi omogenei su tutto il territorio nazionale per il perseguimento delle finalità del Fascicolo Sanitario Elettronico (FSE)**

Criticità sollevate dal Garante riguardo ai contenuti e all'alimentazione dell'EDS:

- ▪ **Indeterminatezza dei contenuti**: Lo schema di decreto non indica chiaramente la tipologia di dati, rendendo i contenuti "indeterminati e indeterminabili".
- ▪ **Ampliamento eccessivo**: La formulazione dell'EDS va oltre quanto previsto dalla normativa primaria. Il Garante ha chiesto di esplicitare la necessità di raccogliere tutte le categorie di dati rispetto alle finalità perseguibili, in base ai principi di proporzionalità e minimizzazione.
- ▪ **Mancanza di chiarezza sulle modalità di alimentazione**: La disposizione non descrive le modalità, ma si limita a indicare che l'alimentazione avviene "utilizzando le funzionalità del Gateway". Il Gateway, tuttavia, è una componente informatica non prevista dalla normativa primaria, ma solo dagli schemi di decreto.
- **Raccolta retroattiva**: Si evidenzia la necessità che siano raccolti soltanto i dati generati *successivamente* all'adozione dello schema di decreto.
- **Inadeguatezza del rinvio**: I trattamenti dell'EDS sono diversi da quelli del FSE per finalità, titolarità e operazioni, rendendo insufficiente un mero rinvio.
- ▪ **Diritto di oscuramento**: Non è chiaro come l'EDS gestisca le richieste di oscuramento o revoca dal FSE, per assicurare l'esattezza e l'aggiornamento dei dati elaborati.
- **Informativa carente**: L'informativa tipo allegata allo schema FSE è "sostanzialmente priva di tutti gli elementi richiesti dagli artt. 13 e 14 del Regolamento" per i trattamenti specifici e delicati dell'EDS.

Criticità sollevate dal Garante:

- **Mancanza di dettagli sul consenso**: Non sono presenti elementi attuativi sull'ambito di operatività del consenso e sulle conseguenze di un'eventuale revoca specifica per l'elaborazione dei dati e l'erogazione dei servizi dell'EDS.
- ▪ **Accesso in emergenza**: Sono state rilevate incongruenze tra i due schemi di decreto riguardo all'accesso in emergenza. In tali casi, l'accesso al FSE dovrebbe essere limitato al Profilo Sanitario Sintetico (PSS) per chi non ha dato il consenso per finalità di cura, e a dati non direttamente identificativi per emergenze sanitarie o di igiene pubblica.
- **Incoerenze e genericità**: Si evidenziano incongruenze tra gli schemi FSE e EDS sui servizi offerti e una "estrema genericità" riguardo ai "Servizi di amministrazione, monitoraggio e controllo".
- ▪ **Principio di proporzionalità**: L'elaborazione dei dati per l'offerta di servizi dovrebbe avvenire solo su specifica richiesta del soggetto autorizzato ad accedervi, per rispettare il principio di proporzionalità. Lo schema non sempre lo specifica.
- ▪ **Mancanza di livelli di accesso diversificati**: Non sono previsti livelli diversificati di accesso al FSE/EDS, il che è essenziale per il principio di minimizzazione dei dati.
- ▪ **Necessità di riformulazione**: Le disposizioni sui servizi necessitano di riformulazione per indicare, per ogni finalità e soggetto, i servizi specifici, la tipologia di dati raccolti ed elaborati, le modalità e le fattispecie di richiesta.

Valutazione d'Impatto sulla Protezione dei Dati (DPIA) e Misure di Sicurezza criticità

- Data la natura su larga scala e ad alto rischio del trattamento dei dati sanitari, è obbligatoria una preventiva Valutazione d'Impatto ai sensi dell'art. 35 del Regolamento.

Incompletezza e imprecisioni: La VIP presentata in "bozza" è incompleta, contiene numerose carenze, imprecisioni e non considera i trattamenti specifici dell'EDS.

Titolarità dei Trattamenti

- Sebbene la normativa primaria individui il Ministero della Salute come titolare del trattamento dell'EDS, lo schema di decreto non definisce chiaramente il perimetro di tale titolarità rispetto agli altri soggetti coinvolti.

- **Mancanza di descrizione dei ruoli**: Lo schema non definisce le operazioni di trattamento delegate ad AGENAS, né descrive i ruoli nelle fasi di raccolta ed elaborazione dei dati e nella richiesta dei servizi.

Il nuovo Decreto EDS pubblicato in Gazzetta Ufficiale il 5 marzo 2025 istituisce :

Modello federato e partecipativo: la legge che rende protagonisti, nella gestione del dato e delle tecnologie, regioni, aziende sanitarie, territori ma sopratutto i medici curanti e i cittadini

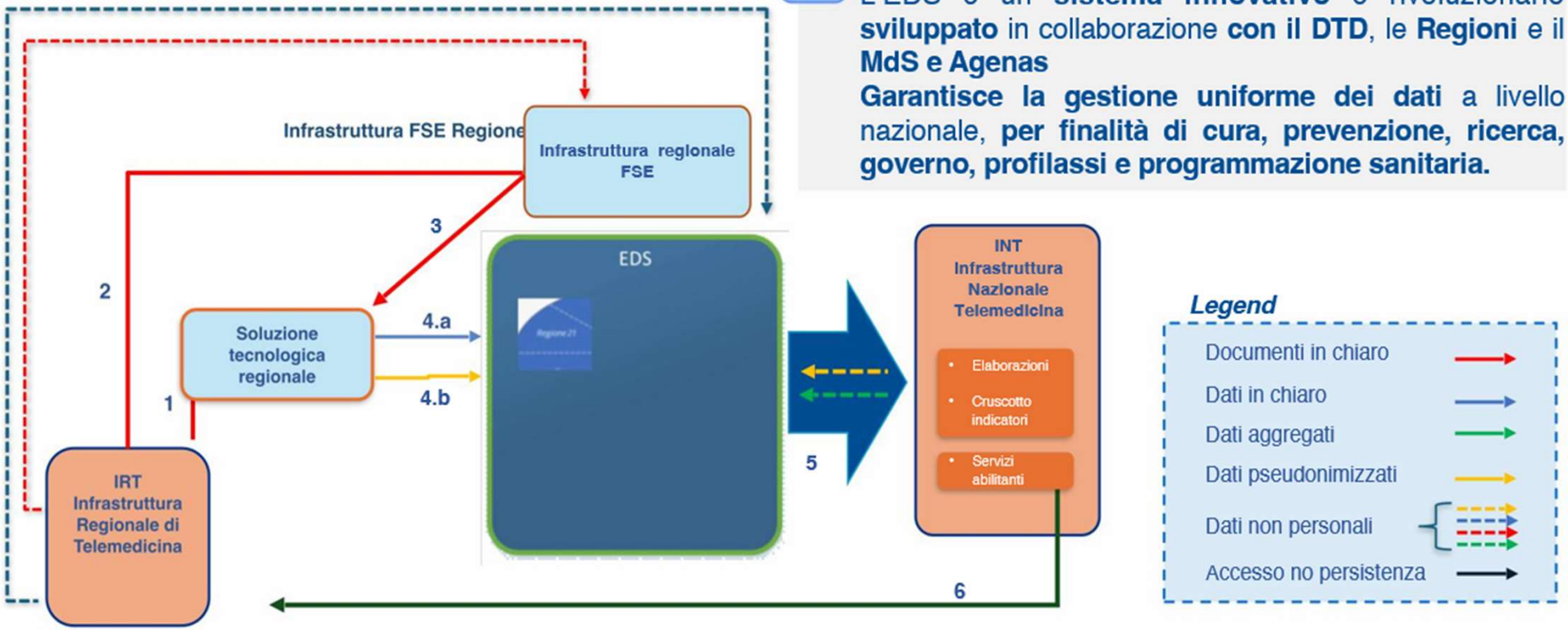
Interoperabilità: il sistema garantisce una totale interoperabilità di tutti i dati clinici che restano nelle strutture sanitarie e nelle regioni dove sono stati generati a garanzia della privacy del cittadino

Sistema informativo nazionale: per la prima volta la sanità ha un sistema informativo basato su dati clinici della persona e della comunità (real world data) standardizzati e non su dati amministrativi

L'EDS garantisce l'integrazione tra i tre pilastri che costituiscono il nuovo medium della sanità voluto dal PNRR: FSE, Telemedicina e AI.

L’EDS è il motore del nuovo sistema di condivisione dei dati clinici CHE ALIMENTA ANCHE LA TELEMEDICINA

L'EDS è un **sistema innovativo** e rivoluzionario **sviluppato** in collaborazione **con il DTD**, le **Regioni** e il **MdS e Agenas**
Garantisce la gestione uniforme dei dati a livello nazionale, **per finalità di cura, prevenzione, ricerca, governo, profilassi e programmazione sanitaria.**



Piattaforma Nazionale di Telemedicina (PNT)

L'architettura della Piattaforma di Telemedicina

L'infrastruttura recupera i dati necessari dal livello regionale, i quali garantiscono l'erogazione dei servizi minimi di telemedicina.

La Piattaforma Nazionale di Telemedicina in ***cloud*** è composta dai seguenti ambienti:

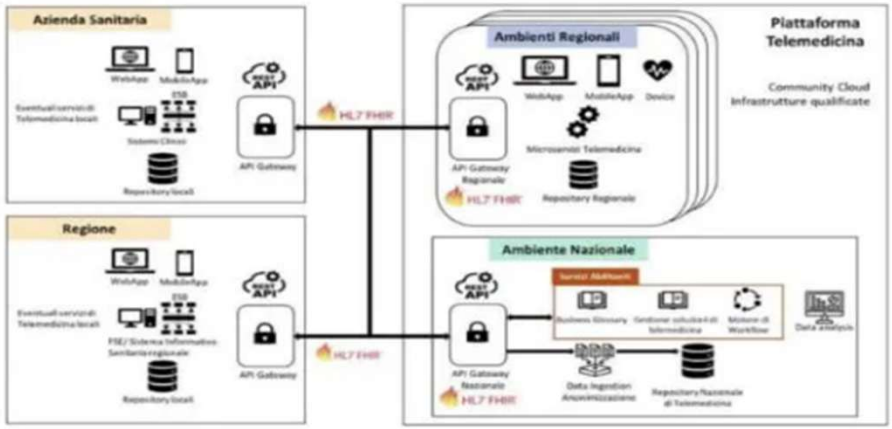
- **Ambiente Nazionale** dedicato ai servizi abilitanti a livello centrale
- **Ambiente Regionale** dedicato ai moduli relativi ai servizi minimi di telemedicina

I moduli principali

Gateway: assicura che i dati e i documenti siano conformi agli standard(HL7 FHIR)- **modulo nuovo**

Ecosistema Dati Sanitari: modulo per la raccolta dei dati ed erogazione di servizi, sia con finalità di cura che di prevenzione- **modulo nuovo**

I servizi minimi di telemedicina previsti sono: **televisita, teleconsulto, teleassistenza, telemonitoraggio**, etc etc.



Piattaforma Nazionale di Telemedicina (PNT)

- È composta da un'infrastruttura nazionale (INT) gestita da Agenas e da 21 infrastrutture regionali (IRT) gestite da Regioni e Province autonome.

- **Infrastruttura Nazionale di Telemedicina (INT)**: Non effettua trattamenti di dati personali (articoli 3, comma 1 e 4 dello schema di decreto), ma fornisce servizi abilitanti per lo sviluppo, l'armonizzazione e il monitoraggio della telemedicina a livello nazionale. Assicura l'interoperabilità delle IRT senza trattare i dati.

- ▪ **Infrastrutture Regionali di Telemedicina (IRT)**: Sono le responsabili dei trattamenti di dati personali, in quanto attraverso di esse vengono erogate le prestazioni sanitarie in telemedicina (articolo 3, comma 2 dello schema di decreto). Le IRT trattano dati, previo consenso dell'assistito, per l'erogazione dei servizi e la conseguente generazione di dati e documenti che saranno poi conferiti al FSE e all'EDS (articolo 3, comma 6 dello schema di decreto). Tuttavia, le IRT non conserveranno i dati e i documenti generati nell'erogazione della telemedicina (articolo 12 dello schema di decreto).

- ▪ **Agenas**: Ha la titolarità per alcune funzioni specifiche, come la valutazione delle tecnologie sanitarie (HTA). Per questo compito, l'EDS renderà disponibili ad Agenas specifici servizi di estrazione di dati previamente elaborati, ai quali Agenas potrà accedere nel rispetto dei principi di minimizzazione, necessità e pertinenza (articoli 2, comma 5, 3 commi 7 e 8 e 8 dello schema di decreto e allegato 2). Il personale di Agenas che accede a flussi di dati pseudonimizzati per altre finalità non accederà ai dati messi a disposizione dai servizi dell'EDS per finalità di governo.

Le tappe di realizzazione del Decreto EDS nel 2025-2026

Sono tre le tappe fondamentali per la realizzazione del Decreto EDS (1/3)

PRIMA TAPPA:
RILASCIO DELLE COMPONENTI CHIAVE GIÀ' IN CORSO
(FEBBRAIO 25)

Attivazione dei Gateway Regionali e Centrali per il trasferimento sicuro dei dati dai sistemi produttori locali all'EDS, garantendo validità e conformità agli standard internazionali

Creazione delle Unità di Archiviazione Regionali (UAR), per gestire i dati sanitari in chiaro, proteggendo la privacy dei cittadini e assicurando l'accesso continuo ai dati

Implementazione del Broker per l'Architettura Federata, garantendo una comunicazione sicura e fluida tra le Regioni e gli operatori sanitari, creando le basi per una sanità digitale moderna

Sono tre le tappe fondamentali per la realizzazione del Decreto EDS (2/3)

SECONDA TAPPA:
ACCESSO SICURO E
ARCHIVIAZIONE PROTETTA

Presto disponibile il layer di servizi per l'accesso sicuro ai dati in chiaro e l'alimentazione delle unità di archiviazione con dati pseudonimizzati e anonimizzati, garantendo massima protezione e sicurezza

L'attivazione di un set completo di servizi avanzati trasformerà l'esperienza di cittadini, medici e Istituzioni

Sono tre le tappe fondamentali per la realizzazione del Decreto EDS (3/3)

TERZA TAPPA:
MIGLIORAMENTO CONTINUO PER UN SISTEMA IN EVOLUZIONE

L'adozione di tecnologie innovative per soddisfare nuove esigenze, ottimizzare le decisioni cliniche e rendere i dati sanitari accessibili e utilizzabili, sfruttando il potenziale di un enorme patrimonio informativo

Tutto questo è raggiungibile con l'introduzione di tecnologie avanzate e strumenti innovativi

Estensione funzionalità EDS

per l'uso di modelli comuni e condivisi tra i professionisti

Introduzione di tecnologie di AI

per l'analisi predittiva e il supporto alle decisioni cliniche

Che effetto avrà sul funzionamento della sanità

Una rivoluzione dell'assistenza sanitaria, con l’EDS riduzione delle liste d'attesa e ottimizzazione delle risorse grazie a dati clinici aggiornati

Storia clinica completa e Patient Summary

L'articolo 4 del DM 7 settembre 2023 individua i contenuti minimi del Fascicolo Sanitario Elettronico (FSE), che includono il profilo sanitario sintetico PSS, contenente la storia clinica del paziente. Il DM Salute del 27 giugno 2025 è un decreto attuativo che fornisce indicazioni sui contenuti del suddetto profilo sanitario sintetico, specificando come questo debba essere compilato e aggiornato per assicurare la continuità delle cure e permettere un rapido inquadramento del paziente.

Dal prossimo 30 settembre, il Fascicolo sanitario elettronico di ogni cittadino sarà completato con un Profilo Sanitario Sintetico (PSS), che sarà redatto e aggiornato dal medico di medicina generale o dal pediatra di libera scelta.
A stabilirlo è il decreto del ministero della Salute del 27 giugno, che è stato pubblicato in Gazzetta Ufficiale lunedì 1° settembre.
Il PSS riassume la storia clinica dell’assistito e la sua situazione attuale e si affianca alle altre informazioni digitalizzate disponibili.
In caso di emergenza, il PSS potrà essere consultato anche senza consenso esplicito dell’assistito, salvo esercizio del diritto di oscuramento dati, per il tempo strettamente necessario ad assicurare cure indispensabili.

Disponibilità dei dati strutturati

Nuovo medium della sanità: FSE, Telemedicina e AI

I RUOLI DI PROTEZIONE DEI DATI PERSONALI

L'individuazione dei ruoli privacy (Titolare, Responsabile, Contitolare) è un processo che richiede una **valutazione sostanziale e non meramente formale dei trattamenti di dati**, da condurre "case by case" in ottemperanza ai principi di **accountability e privacy by design**.

Avremo il :

Ruolo delle Regioni e delle Piattaforme/Sistemi Informativi

La determinazione del ruolo della Regione dipende dalle specifiche attività di trattamento che essa svolge.

1)Regione come Titolare del Trattamento: Si configura uno scenario in cui la Regione è **titolare del trattamento se definisce il processo di identificazione dell'assistito sulla piattaforma**, ma limitatamente a tali specifici trattamenti. Questa valutazione richiede un'analisi caso per caso.

2) **Regione come Responsabile del Trattamento:** Con riferimento alla **gestione tecnica e informatica della piattaforma**, l'ente del sistema sanitario regionale (come l'ASL) è il titolare dei dati dei propri assistiti, e **alla Regione va attribuito il ruolo di responsabile**. In questo caso, il Titolare (ASL) ha il compito di accettare e valutare le politiche di sicurezza condivise dalla Regione e può richiedere ulteriori misure se necessarie, che il Responsabile (Regione) è tenuto a implementare.

3)Le questioni chiave relative al ruolo delle Regioni quando mettono a disposizione piattaforme/sistemi informativi per i diversi Enti del sistema sanitario regionale sono state sollevate anche dalla Deliberazione del Garante Privacy del 4 giugno 2015 Dossier Sanitario

Ruoli di Protezione dei Dati Personali: le Societa’ in House

4) Ruolo delle Società in House

- Le società in house che sviluppano servizi tecnici per la sanità, come applicazioni per il Fascicolo Sanitario Elettronico (FSE), sistemi di prenotazione o pagamento, si configurano **nella maggior parte dei casi quale Responsabile del trattamento**. Anche qui, vale il principio della valutazione "case by case". Il Garante ha in passato sanzionato sia Regioni che società in house per violazioni legate alla mancata designazione o a misure di sicurezza inadeguate. Un esempio significativo è il **Provvedimento del 27 novembre 2024 (doc. web n. 10095810)**, in cui sono stati sanzionati più soggetti a seguito di una violazione di dati personali dovuta a un bug di sicurezza nel sistema di autenticazione del portale FSE di una Regione:
- ▪ La **Regione è stata sanzionata come titolare del Portale** per la violazione dei principi di integrità e riservatezza, e di protezione dei dati fin dalla progettazione e per impostazione predefinita.
- ▪ La **società in house è stata sanzionata in qualità di responsabile dell’attività di implementazione tecnica del FSE**, per non aver implementato misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio.
- ▪ Un **sub-responsabile** (responsabile della progettazione e realizzazione tecnica del sistema informatico) è stato sanzionato per non aver implementato misure adeguate e per non averne regolarmente testato l'efficacia.

Ruoli nelle Aggregazioni Funzionali Territoriali

- Le AFT sono **"forme organizzative mono-professionali che condividono, in forma strutturata, obiettivi e percorsi assistenziali"**. Esse consentono, nel rispetto della normativa sulla privacy e della sicurezza nella gestione dei dati, l'accesso di ogni medico della AFT a informazioni cliniche degli assistiti degli altri medici operanti nella medesima AFT. L'Accordo Collettivo Nazionale (ACN) attuale non affronta gli aspetti di protezione dei dati personali, inclusi i ruoli e il presupposto di liceità che permetterebbe ai medici di trattare i dati dei pazienti in condivisione. Si auspica che la prossima contrattazione possa affrontare tali aspetti.

- In assenza di chiare indicazioni normative, l'attribuzione dei ruoli deve essere basata sul **modello di AFT previsto a livello territoriale**, tenendo conto dei mezzi di trattamento e del rapporto fiduciario medico-paziente. In concreto, le opzioni potrebbero includere:
  - Un rapporto di **contitolarità tra i diversi medici**.
  - Una **titolarità autonoma**.

- Entrambe le opzioni hanno **impatti differenti in termini di obblighi informativi e di esercizio dei diritti degli interessati**. Rimane fermo il principio della pertinenza delle informazioni a cui si può accedere, necessarie per l'espletamento delle proprie funzioni istituzionali dei diversi soggetti. I ruoli nelle AFT sono stati oggetto di indagine da parte del Garante Privacy.

Deliberazione del Garante Privacy del 4 giugno 2015 dossier sanitario più tutele per i pazienti : consenso informato, accessi tracciati, immediata comunicazione dei data breach.

Il dossier sanitario, ha introdotto **maggiori tutele per i pazienti**. Queste tutele sono strettamente connesse alla corretta gestione dei ruoli privacy e dei trattamenti di dati:

- **Consenso Informato:** I pazienti devono avere la possibilità di scegliere liberamente se far costituire o meno il dossier sanitario. L'assenza di consenso non deve pregiudicare l'accesso alle cure. Per informazioni particolarmente delicate (es. HIV, interruzioni di gravidanza), è richiesto un consenso specifico.
- **Informazione Chiara:** La struttura sanitaria deve informare il paziente in modo trasparente su chi avrà accesso ai suoi dati e quali operazioni saranno compiute.
- **Diritti del Paziente:** Deve essere garantito l'esercizio dei diritti (accesso, integrazione, rettifica), la conoscenza di ogni consultazione del dossier (reparto, data, orario) e la possibilità di **"oscurare" alcuni dati o documenti sanitari**.
- **Sicurezza dei Dati:** Sono richieste elevate misure di sicurezza, inclusa la separazione dei dati sulla salute da altri dati personali e la definizione di criteri per la cifratura dei dati sensibili.
- **Accessi Tracciati e Limitati:** L'accesso al dossier è consentito solo al personale sanitario coinvolto nella cura, e **ogni accesso e operazione deve essere tracciato e registrato in file di log**, conservati per almeno 24 mesi.
- **Comunicazione dei Data Breach:** Le strutture sanitarie hanno l'obbligo di comunicare immediatamente all'Autorità (entro 48 ore dalla conoscenza del fatto) le violazioni o incidenti informatici che possano avere un impatto significativo sui dati.

In sintesi, la corretta identificazione e attribuzione dei ruoli privacy nel settore sanitario è fondamentale per garantire la protezione dei dati personali, rispettare il principio di accountability e assicurare la sicurezza delle informazioni sanitarie, con implicazioni dirette sulle responsabilità delle diverse entità e sui diritti dei pazienti.

Aspetti Chiave del Sistema EDS (European Data Space)

Il 5 marzo 2025 il regolamento sullo spazio europeo dei dati sanitari è stato pubblicato ufficialmente nella Gazzetta ufficiale dell'Unione Europea. Entra in vigore il 26 marzo 2025 e segna l'inizio della fase di transizione verso la piena attuazione.

- Il documento introduce due aspetti fondamentali relativi all'European Data Space (EDS):
- la **circolazione libera e sicura dei dati tra i settori e gli Stati membri dell'UE**, garantendo al contempo la protezione della privacy e dei diritti dei cittadini tramite norme consolidate. Gli EDS mirano a creare un mercato unico dei dati, supportando imprese, ricercatori e amministrazioni pubbliche nell'accesso e nel riutilizzo dei dati, promuovendo così l'innovazione e una società guidata dai dati.
  Interoperabilità Europea e Profilassi Internazionale: "L'architettura dell'EDS è conforme alle normative europee, in particolare al regolamento sullo Spazio Europeo dei Dati Sanitari." Questo sistema "consente di condividere selettivamente i dati con i sistemi di sorveglianza epidemiologica dell'UE e dell'OMS, in linea con il Regolamento Sanitario Internazionale." L'adozione dello standard **FHIR** "garantisce la compatibilità con iniziative sanitarie internazionali, creando un'infrastruttura per la condivisione rapida e sicura di informazioni in contesti di emergenza, come appreso dalla pandemia di COVID-19." EHDS si basa su una strategia complessiva per i dati dell'UE, definendo regole e standard comuni per l'interoperabilità dei sistemi sanitari e la gestione dei dati.
- Viene creato un ambiente di dati specifico per la salute, che include l'infrastruttura digitale MyHealth@EU per l'accesso transfrontaliero a dati sanitari e HealthData@EU per il riutilizzo dei dati per scopi di ricerca e innovazione.
- Ogni Stato membro designerà autorità responsabili dell'attuazione delle nuove disposizioni.

Considerazioni Finali

- La gestione della protezione dei dati nel settore della sanità digitale è un compito complesso che richiede un'analisi dettagliata e flessibile dei ruoli basata sul principio di accountability e privacy by design. L'esperienza ha dimostrato che le violazioni possono coinvolgere tutti i livelli della catena di responsabilità, rendendo cruciale l'implementazione di misure di sicurezza adeguate e costantemente testate.

- L'evoluzione verso l'EDS e l'interoperabilità europea introduce nuove sfide e opportunità per la condivisione sicura dei dati, mantenendo al contempo un forte focus sulla tutela dei diritti degli interessati.

Grazie per l'attenzione!