



***CONSULENZA PROFESSIONALE NORMATIVA E
TECNICA PER LA GESTIONE DELL'IMPRESA***

Fascicolo sanitario elettronico, cos' è? Cosa contiene?



Si ricorda che i documenti sanitari relativi alle prestazioni a cui si può avere accesso in anonimato non alimentano il FSE (dati e documenti disciplinati dalle norme a tutela delle persone sieropositive, delle donne che si sottopongono a un'interruzione volontaria di gravidanza, delle vittime di atti di violenza sessuale etc.)

Cosa è?

Il Fascicolo Sanitario Elettronico (FSE) è lo strumento attraverso il quale il cittadino può tracciare e consultare tutta la storia della propria vita sanitaria, condividendola con i professionisti sanitari per garantire un servizio più efficace ed efficiente. Le informazioni presenti nel Fascicolo del cittadino vengono fornite e gestite dalle singole regioni.

Cosa contiene?

Il fascicolo, normato dal D. P. C. M. n° 178 del 2015, a partire dal 19 maggio 2020, è alimentato, in maniera continuativa e tempestiva dai soggetti e dagli esercenti le professioni sanitarie, anche privati, , con i dati degli eventi clinici relativi all'assistenza sanitaria ricevuta: attestazioni vaccinali anti-COVID-19, promemoria di prenotazione visite, verbali di pronto soccorso, lettere di dimissioni ospedaliere, profilo sanitario sintetico, consenso o diniego alla donazione degli organi e tessuti, prescrizioni farmaceutiche, piani diagnostico-terapeutici.

Fascicolo sanitario elettronico, cos' è? Cosa contiene?

Il FSE persegue tre finalità:

- 1) finalità di cura (prevenzione, diagnosi, cura e riabilitazione);
- 2) finalità di ricerca (studio e ricerca scientifica in campo medico, biomedico ed epidemiologico);
- 3) finalità di governo (programmazione sanitaria, verifica della qualità delle cure e valutazione dell'assistenza sanitaria).



L'interessato deve esprimere il consenso?

L'assistito deve esprimere un consenso, valido una tantum e sempre revocabile, per permettere al personale sanitario che lo ha in cura di accedere al suo FSE. Anche se l'assistito non dà il consenso, la prestazione sanitaria gli è comunque garantita.

Recentemente, il FSE è stato semplificato per essere automaticamente alimentato. Questo permette all'assistito di consultare facilmente i propri documenti socio-sanitari, anche quelli provenienti da strutture sanitarie fuori dalla propria Regione, grazie all'interoperabilità del Sistema Tessera Sanitaria.

Gli organi di governo sanitario possono accedere ai dati pseudonimizzati presenti nel FSE per compiere le loro funzioni istituzionali (come la programmazione delle cure e la gestione delle emergenze sanitarie), indipendentemente dal consenso dell'assistito.

Chi può accedere al FSE?



- L'assistito, che potrà così consultare i propri documenti sanitari sia clinici che amministrativi, come le ricette o i certificati di malattia.
- Con il consenso dell'assistito, tutti gli esercenti le professioni sanitarie (pubblici e privati) che intervengono nel processo di cura dell'assistito, compreso il medico di base, cui compete anche il compito di redigere il patient summary (profilo sanitario sintetico).
- Le Regioni e il Ministero della salute per finalità di governo e di ricerca (senza i dati identificativi diretti dell'assistito e nel rispetto dei principi di indispensabilità, necessità, pertinenza e non eccedenza).

Chi non può accedere al FSE?

I periti, le compagnie di assicurazione, i datori di lavoro, le associazioni scientifiche e gli organismi amministrativi pur se operanti in ambito sanitario, e comunque i terzi non autorizzati non possono accedere al FSE.

DIRITTO DI OSCURAMENTO

L'interessato ha il diritto di richiedere l'oscuramento dei dati e dei documenti sanitari e sociosanitari sia prima dell'alimentazione del FSE sia successivamente.



Obblighi della struttura sanitaria

1. Fornire all'interessato una specifica informativa privacy sulle caratteristiche del servizio di FSE, ai sensi dell'art. 13 del GDPR e di richiedergli un apposito consenso per il trattamento dei dati personali connessi a tale servizio. Ad oggi, il sistema è costruito in modo da lasciare traccia dell'identità del soggetto che accede al FSE, nonché di colui che immette informazione all'interno dello stesso fascicolo
2. Prevedere idonee misure di sicurezza.



► Dossier sanitario Elettronico

► Cos'è e quali differenze ci sono con il FSE?

Il dossier sanitario elettronico è lo strumento costituito presso un'unica struttura sanitaria (ospedale, azienda sanitaria, casa di cura) che raccoglie informazioni sulla salute di un paziente al fine di documentarne la storia clinica presso quella singola struttura e offrirgli un migliore processo di cura.

Si differenzia dal fascicolo sanitario elettronico in cui invece confluisce l'intera storia clinica di una persona generata da più strutture sanitarie.

► Dossier sanitario Elettronico



Accesso Limitato:
L'accesso ai dati è strettamente limitato al personale sanitario autorizzato, garantendo la riservatezza e la protezione dei dati del paziente.

Consenso dell'Assistito:
Il consenso informato dell'assistito è fondamentale. Deve essere specifico per l'accesso al dossier e può essere revocato in qualsiasi momento.

Trasparenza e Informazione:
Gli assistiti devono essere adeguatamente informati su come i loro dati vengono gestiti e su come possono esercitare i loro diritti in relazione ai dati stessi.

Sicurezza dei Dati:
Misure rigorose per garantire la sicurezza dei dati, proteggendoli da accessi non autorizzati, perdite o alterazioni.

Limitazione della Conservazione:
I dati devono essere conservati solo per il tempo necessario agli scopi per cui sono stati raccolti.

Diritto di Accesso e Correzione:
Garantire agli assistiti il diritto di accedere ai loro dati e richiederne la correzione in caso di errori.

Interoperabilità e Compatibilità:
Assicurare che il sistema sia interoperabile a livello nazionale e compatibile con altri sistemi sanitari, rispettando sempre le normative sulla privacy.

L'obiettivo è bilanciare l'efficienza della gestione dei dati sanitari con la tutela rigorosa della privacy e dei diritti dei pazienti.

La struttura sanitaria deve:

Garantire al paziente l'esercizio dei diritti (accesso ai dati, integrazione, rettifica, etc.) e la possibilità di conoscere il reparto, la data e l'orario in cui è avvenuta la consultazione del suo dossier.

Garantire al paziente la possibilità di "oscurare" alcuni dati o documenti sanitari che non intende far confluire nel dossier.

Adottare elevate misure di sicurezza.

I dati sulla salute dovranno essere separati dagli altri dati personali, e dovranno essere individuati criteri per la cifratura dei dati sensibili.

L'accesso al dossier sarà:

Consentito solo al personale sanitario coinvolto nella cura.

Ogni accesso e ogni operazione effettuata, anche la semplice consultazione, saranno tracciati e registrati automaticamente in appositi file di log che la struttura dovrà conservare per almeno 24 mesi.

Comunicare al Garante eventuali violazioni di dati o incidenti informatici

(data breach) entro quarantotto ore dalla conoscenza del fatto.

Prevedere una informativa specifica e la corretta acquisizione di uno specifico consenso



Dispositivi medici o elettromedicali: impatto sulla protezione dei dati personali



E' importante per le strutture sanitarie adottino un approccio organizzativo basato sui principi del GDPR, garantendo la sicurezza dei dati trattati dai dispositivi medici e dimostrando la conformità attraverso pratiche di accountability. Questo processo richiede una stretta collaborazione tra gli esperti della data protection e le diverse figure professionali all'interno delle strutture sanitarie.



particolare attenzione ai dispositivi medici e ai loro requisiti per garantire la protezione dei dati personali



I principi chiave del GDPR, come la limitazione della conservazione, la minimizzazione dei dati e la responsabilizzazione, sono fondamentali nella gestione dei dispositivi medici. Questi ultimi, spesso integrati in sistemi complessi, trattano dati personali e sensibili dei pazienti e devono garantire la sicurezza nella trasmissione e conservazione dei dati.



Una problematica principale è la duplicazione dei dati: anche se trasmessi ai sistemi centralizzati, possono rimanere memorizzati nei dispositivi stessi, aumentando il rischio di sicurezza.



Si raccomanda quindi che i dispositivi, dopo aver inviato i dati, siano cancellati definitivamente, lasciando la conservazione e la gestione dei dati ai server centralizzati del sistema informativo ospedaliero (SIO).



Per i dispositivi medici "stand alone" non integrati nel SIO, che sono sempre meno utilizzati, si richiedono procedure di gestione dei dati differenti, con maggiori controlli e misure di sicurezza.



Dal punto di vista della data protection, le strutture sanitarie devono monitorare attentamente tutti i dispositivi, classificandoli e tenendo un registro aggiornato che includa dettagli come la tipologia, l'ubicazione, la categoria di dati raccolti e le tempistiche di cancellazione..

▶ *Grazie per l'attenzione*

- ▶ *Dott.ssa Michela Giannetta – Privacy Legal & compliance Consultant*

Urbano Consulting Group S.r.l.

▶ *Via Lima n.7*

▶ *Roma, 00198*

▶ *Cel.: +39 3317877164*

▶ *e-mail: info@uc-group.it*

▶ **SERVIZI**

▶ *Legislazione Sanitaria e Healthcare*

▶ *Protezione dei dati personali*

▶ *DPO (Data Protection Officer)*

▶ *Salute e Sicurezza sui Luoghi di Lavoro*