# Il Fascicolo Sanitario Elettronico: tra consenso e misure di sicurezza

Le organizzazioni operanti nel settore sanitario hanno assistito negli ultimi anni a una rivoluzione tecnologica e normativa.

Il progressivo passaggio dal cartaceo al digitale, spesso avvenuto in maniera disordinata, ha accentuato la fragilità delle organizzazioni healthcare dal punto di vista della sicurezza informatica - ciò è avvenuto in un contesto normativo nel quale la direttiva NIS da una parte, e il GDPR dall'altra pongono ulteriori obblighi di compliance agli operatori del settore sanitario.

Nei paragrafi che seguono si offrirà una panoramica sulle novità in materia di Fascicolo Sanitario Elettronico (FSE) a seguito dell'introduzione del GDPR e del decreto di adeguamento al nostro Codice in materia di protezione dei dati personali.

## Il trattamento di dati sanitari

Il trattamento dei dati sanitari, ovvero quelli "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", è consentito solo nel caso in cui il trattamento sia necessario per alcuni motivi tassativamente individuati dalla normativa. In tutte le altre ipotesi, il trattamento richiede il consenso esplicito dell'interessato.

Facciamo chiarezza, non è necessario il consenso se il trattamento è svolto per:

**- Motivi di interesse pubblico rilevante sulla base del diritto dell'Unione** o degli stati membri, ad esempio:

- trattamenti effettuati da soggetti che svolgono compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione;
- trattamenti effettuati dalla protezione civile.

**- Motivi di interesse pubblico nel settore della sanità pubblica**, ad esempio:

- I trattamenti di dati necessari alla protezione da gravi minacce per la salute a carattere transfrontaliero (ad esempio, a questa base giuridica si riconduce la misurazione della temperatura corporea negli aeroporti);
- Trattamenti necessari a garantire la qualità e sicurezza dell'assistenza sanitaria, dei medicinali e dei dispositivi medici.

**- Finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali («finalità di cura»)** sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità (art. 9, par. 2, lett. h) e par. 3 del Regolamento e considerando n. 53) effettuati sotto la responsabilità di un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza.

I trattamenti che non rientrano nelle ipotesi sopra descritte richiedono sempre il **consenso esplicito** dell'interessato: tale consenso esplicito è oggi richiesto anche per la formazione e alimentazione del Fascicolo sanitario elettronico.

## Il fascicolo sanitario elettronico

In questo momento di difficoltà dovuto alla pandemia Covid-19, moltissime strutture hanno implementato un fascicolo sanitario elettrico, per consentire la consultazione dei referti e delle prenotazioni online, senza necessità di uscire di casa e consentire così una erogazione del servizio sanitario sicuro con le raccomandazioni delle autorità,

Il FSE è “l’insieme dei dati e dei documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi riguardanti l’assistito, nell’ambito di tutte le strutture sanitarie nazionali (anche private), istituito da regioni e province autonome”.

Il Fascicolo Sanitario elettronico può contenere i dati relativi a eventi clinici che si sono verificati in qualsiasi struttura del territorio (nazionale o locale) e può essere aggiornato o modificato da ciascun medico operante in tutta la penisola.

Inoltre, attraverso il FSE è possibile consultare molti documenti sanitari rilevanti, come ad esempio le prescrizioni mediche e farmaceutiche, le prenotazioni, le cartelle cliniche, i referti anche di pronto soccorso, le schede di dimissioni ospedaliere, i certificati medici e le esenzioni.

Il FSE è uno strumento molto utile alle organizzazioni sanitarie, il quale consente la tutela del paziente rendendo i dati sanitari sempre disponibili agli operatori addetti.

Al fine di essere uno strumento efficace, però, è necessario che i dati presenti nel FSE siano non solo disponibili, ma anche integri (cioè corretti, aggiornati e non modificabili da soggetti non autorizzati) e riservati (cioè accessibili unicamente ai soggetti autorizzati). Raggiungere gli obiettivi di riservatezza, integrità e disponibilità dei dati contenuti nei Fascicoli sanitari elettronici non è cosa banale, e richiede l’adozione di misure di sicurezza adeguate – così come richiesto dal GDPR (e non solo, come vedremo successivamente).

Oltre a ciò, è necessario prestare attenzione a un altro aspetto fondamentale: la gestione del consenso esplicito alla formazione del FSE.

## Il consenso per il trattamento dei dati tramite FSE

Il consenso alla creazione e alimentazione del FSE è **autonomo e distinto** rispetto al trattamento dei dati al fine di eseguire la prestazione sanitaria in sé.
Concettualmente è quindi necessario distinguere tra il trattamento di dati necessario alla cura del paziente (che sarà sostenuto da una delle condizioni che abbiamo individuato all'inizio, es. la "finalità di cura") e il trattamento dei dati relativo alla creazione e alimentazione del Fascicolo Sanitario Elettronico (per il quale deve necessariamente aversi il consenso esplicito del paziente – così come indicato dal nostro Garante).
Infatti, potrebbe accadere che un paziente voglia essere curato ma non voglia che si crei un Fascicolo Sanitario Elettronico a suo nome, potenzialmente accessibile agli operatori sanitari di tutta Italia e contenente le sue informazioni particolarmente sensibili (compresi, ad esempio, la positività a malattie sessualmente trasmissibili, la presenza di problemi genetici, l'eventualità che il paziente abbia ricevuto cure psichiatriche, etc.). In questo caso, al paziente sarà erogata la prestazione sanitaria sulla base degli esami diagnostici prodotti al momento o procurati dal paziente stesso.
Anche l'Autorità Garante per la Protezione dei Dati Personali ha sottolineando che la prestazione sanitaria deve essere comunque garantita anche in caso di mancato consenso al FSE, altresì precisando che il consenso può essere reso *una tantum* e deve essere sempre revocabile.

Lo stesso Garante ritiene possibile, alla luce del contesto normativo mutuato a seguito dell'introduzione del GDPR, una futura modifica del quadro normativo in ordine all'eliminazione della necessità di acquisire il consenso dell'interessato.
In altre parole, si tratterebbe di una estensione dell'ambito di applicazione delle condizioni legittimanti di cui alle lettere g), h), i) dell'art. 9 GDPR.

I recenti interventi di semplificazione consentono che il FSE venga automaticamente alimentato, in modo che lo stesso assistito possa facilmente consultare i propri documenti socio-sanitari, anche se generati da strutture sanitarie situate al di fuori della Regione di appartenenza, grazie all'interoperabilità assicurata dal Sistema Tessera Sanitaria.

Ricordiamo che, a prescindere dal consenso dell'assistito, gli organi di governo sanitario, come il Ministero della salute o le Regioni, possono accedere a dati pseudonimizzati presenti nel FSE per svolgere le relative funzioni istituzionali, ad esempio la programmazione delle cure e la gestione delle emergenze sanitarie.

Se da un lato il Fascicolo Sanitario Elettronico si rivela uno strumento particolarmente utile ai fini di una gestione più efficiente del paziente, dall'altro la sua utilizzazione implica un rilevante impatto sotto il profilo del trattamento dei dati personali. Tra le problematiche relative alla gestione del consenso si trovano gli adempimenti successivi all'esercizio del diritto di "revoca del consenso" da parte del paziente, il quale comporterebbe l'interruzione dell'aggiornamento del fascicolo in base al mutamento del quadro clinico-sanitario del paziente e l'impossibilità per i professionisti sanitari precedentemente autorizzati di consultare i dati integranti il Fascicolo stesso.

## L'informativa

Altra criticità derivante dall'obbligo di acquisire il consenso deriva dalla necessità che l'organizzazione sanitaria abbia reso all'interessato l'**informativa** idonea a comprendere finalità e modalità di trattamento circa i dati sanitari (così come previsto dall'art. 13 del GDPR).

L'omissione di informativa o la presenza di un'informativa inidonea - ad esempio non redatta con linguaggio semplice e comprensibile (che impedisce di fatto la possibilità di esprimere un consenso valido) – comporta un grave rischio sanzionatorio per le organizzazioni del settore sanitario.

Alle sanzioni inflitte dal Garante, dobbiamo aggiungere anche il rischio relativo a eventuali risarcimenti richiesti dagli interessati. Tale eventualità è assolutamente concreta, trattandosi di dati particolarmente sensibili il cui trattamento potrebbe esporre gli interessati a conseguenze gravissime.

## Quali misure di sicurezza adottare?

Il GDPR non impone delle misure di sicurezza specifiche per quanto riguarda i trattamenti effettuati tramite FSE, coerentemente con l'impostazione per la quale è responsabilità del titolare del trattamento (l'organizzazione sanitaria) stabilire quali siano le misure di sicurezza adeguate al rischio.

C'è da rilevare che il nuovo art. 2-septies del Codice in materia di protezione dei dati personali stabilisce che il trattamento di dati sanitari debba avvenire rispettando quanto previsto dalla normativa privacy e, inoltre, "in conformità alle misure di garanzia disposte dal Garante".

Tali "misure di garanzia disposte dal Garante" dovrebbero essere delle indicazioni circa il trattamento dei dati genetici, biometrici e relativi alla salute che il nostro Garante dovrebbe approvare e pubblicare con cadenza biennale – esse dovrebbero indicare anche le misure di sicurezza da adottare.

La nostra Autorità non ha ancora provveduto a disporre tali misure di garanzia e, seppure possiamo aspettarci delle novità in materia, ad oggi non ci resta che affidarci al buon senso.

Vista la particolare sensibilità dei dati archiviati nel FSE, per fronteggiare la "minaccia" delle sanzioni è necessario adottare le misure di sicurezza necessarie a garantire:

1. la certezza dell'origine dei dati;
2. la correttezza ed attualità degli stessi;
3. l'accessibilità agli stessi da parte di soggetti specificamente legittimati.

Poiché la creazione del FSE ha come obiettivo rendere i servizi sanitari più efficienti per i pazienti, è necessario tenere in considerazione il **corretto bilanciamento tra efficienza dei servizi sanitari e tutela dei dati personali**.

Ricordiamo che per l'utilizzo del FSE non è sufficiente possedere la licenza di un software (on premises o in cloud) adatto allo scopo, ma è necessario utilizzare protocolli di comunicazione sicuri ed end-point adeguatamente protetti. Devono essere adottati specifici accorgimenti tecnici per garantire idonei livelli di sicurezza sui tre livelli principali relativi alla sicurezza delle informazioni: le persone, i processi e la tecnologia.

Deve essere effettuata una corretta analisi dei rischi che tenga conto almeno:

- dei rischi di accesso abusivo al sistema informativo relativo al FSE;
- dei rischi di furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi.

Ciò potrà indirizzare l'implementazione di misure di sicurezza come la crittografia.

È importante inoltre che siano sempre assicurati:

- idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (principio del need to know);
- policy, processi e procedure che consentano la verifica periodica della coerenza dei profili di autorizzazione assegnati (c.d. provisioning);
- una elevata confidenzialità ed una protezione più elevata dei dati idonei a rivelare lo stato di salute e la vita sessuale rispetto agli altri dati personali;
- tracciabilità degli accessi e delle operazioni effettuate (Log);
- sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

## Conclusione

Per una organizzazione operante nell'ambito sanitario l'adozione di un fascicolo sanitario elettronico è senza dubbio un elemento di qualità ed efficienza nella gestione dei dati clinici dei pazienti. Tuttavia, il FSE richiede un impegno specifico in relazione non solo alla corretta scelta del fornitore, che dovrà essere attento a queste tematiche e aver progettato la propria soluzione avendo in mente le regole per una corretta privacy by design, ma anche nella gestione della sicurezza delle informazioni "al di fuori" del fascicolo, adottando una governance che risulti sempre adeguata sia alle normative che al contesto delle minacce cibernetiche.

In altre parole, l'implementazione di policy, processi e procedure dedicati a consentire l'accessibilità ai dati solo dalle persone legittimate, la verifica periodica degli accessi e delle operazioni effettuate e livelli di sicurezza adeguati alle minacce ed ai rischi riscontrabili, sono tutte attività di governance che devono essere progettate e realizzate in modo preciso e adatto alla realtà considerata.

LUTECH

With technology
and market driven end-to-end services
we enable Clients to work easier,
reaching their goals
and evolving their business.

info@lutech.it +39 02 2542 7011

**www.lutech.group**