Allegato A

Procedura semplificata per l'erogazione dei farmaci "Dema4All"

Sommario

1. Premessa

La ricetta dematerializzata trova la propria disciplina nel Decreto del Ministero dell'Economia e delle Finanze del 2 novembre 2011 n. 264 avente ad oggetto "De-materializzazione della ricetta medica cartacea, di cui all'articolo 11, comma 16, del decreto-legge n. 78 del 2010".

Sino al 31 dicembre 2022, per l'erogazione delle prescrizioni farmaceutiche è applicata la disciplina prevista per la fase emergenziale da Pandemia Covid.

A partire dal 01 gennaio 2023, invece, la norma prevede che l'assistito possa recuperare il "promemoria dematerializzato" (contenente il Numero della Ricetta Elettronica (NRE)) necessario per ottenere le prescrizioni attese presso la rete delle farmacie, attraverso i seguenti canali:

a) nel portale del Sistema di Accoglienza Centrale (SAC) (www.sistemats.it), anche tramite i sistemi di accoglienza regionali;
b) nel Fascicolo Sanitario Elettronico, di cui all'art. 12 del decreto-legge n. 179/2012;
c) posta elettronica;
d) short message service (SMS).

Tali modalità di trasmissione del NRE, mostrano, tuttavia, alcuni limiti, come di seguito rappresentato.

2. Finalità del documento

Le modalità di recupero del NRE previste dalla norma possono dare un forte impulso al processo di digitalizzazione dei servizi sanitari, tuttavia, sono in grado di determinare anche l'acuirsi della distanza tra i servizi digitali e i cittadini a rischio di esclusione, ovvero, del cosiddetto *digital divide*.

La normativa attuale prevede la necessaria interazione dell'assistito con uno strumento (smartphone o pc) oppure l'ordinaria modalità cartacea. Nel nostro paese, secondo i più recenti dati ISTAT la percentuale di persone che non hanno utilizzato la rete internet nell'arco di tre mesi è pari a 32,1%. Tra l'altro, le categorie di persone maggiormente sensibili al digital divide si collocano nella fascia di età 65-74 anni e 75 anni e più, le quali più cospicuamente si avvalgono dei servizi della rete delle farmacie.

La Regione Emilia-Romagna ha avviato un percorso per assorbire la distanza fra i servizi digitali e la cittadinanza; ovvero, i servizi devono conformarsi ai principi di inclusione e accessibilità. I servizi digitali vanno disegnati in modo da impattare positivamente sul più elevato numero possibile di soggetti. Costituisce misura di buona amministrazione, nonché di rilevante interesse pubblico, superare le interazioni non necessarie tra l'assistito e le piattaforme a mezzo delle quali è governato il sistema sanitario regionale, ovviamente nel pieno rispetto della normativa in materia di protezione dei dati personali.

In tal senso, le farmacie rappresentano, insieme ai medici di medicina generale, un punto di riferimento del SSN sul territorio e possono svolgere un ruolo primario, anche in ragione del rapporto fiduciario con gli assistiti, nelle attività di trattamento di seguito descritte.

Giova preliminarmente sottolineare che il presente servizio risponde a finalità e crismi manifestamente distinti dal Dossier farmaceutico di cui all'art. 12, comma 2-bis, del D.lgs. 179/2012, il quale prevede che "*Per favorire la qualità, il monitoraggio, l'appropriatezza nella dispensazione dei medicinali e l'aderenza alla terapia ai fini della sicurezza del paziente, è istituito il dossier farmaceutico quale parte specifica del FSE, aggiornato a cura della farmacia che effettua la dispensazione*".

D'altra parte, la finalità del servizio Dema4All è quella di definire che l'assistenza farmaceutica, per conto delle unità sanitarie locali del territorio, da parte delle farmacie sia possibile a mezzo della mera presentazione del codice fiscale da parte degli assistiti:

- agevolando le farmacie nell'esercizio della finalità di cura svolta dai farmacisti e consentendo agli assistiti l'approvvigionamento di farmaci riducendo i rischi correlati all'assembramento presso gli ambulatori medici con una soluzione che superi le criticità correlate al Digital Divide;

- promuovendo una soluzione coerente con la centralità del FSE nelle politiche sanitarie digitali.

Alla luce di ciò, il presente documento declina la Procedura semplificata per l'erogazione di farmaci, previa acquisizione del codice fiscale dell'assistito, acquisendo NRE attraverso il FSE o altre modalità.

3. Il FSE

Il D.lgs. 179/2012, come modificato dal D.L. 34/2020, all'art. 12 definisce il Fascicolo sanitario elettronico come "l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, riferiti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale".

Coerentemente il D.lgs. 179/2012, sopra richiamato, l'alimentazione del FSE avviene automaticamente per tutti i cittadini senza necessità di esperire apposito consenso. In tal modo, il Fascicolo Sanitario è naturalmente la piattaforma su cui disegnare i servizi di cura degli assistiti.

3.1 Le finalità di trattamento nel FSE

Al comma 2 dell'art. 12 del D.Lgs. 179/2012 sono definite le finalità per cui possono essere trattati i dati raccolti nel FSE, ovverosia:

a) prevenzione, diagnosi, cura e riabilitazione;

b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico;

c) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria.

Nel caso di specie, il servizio Dema4all assolve alle finalità di cui alla precedente lettera a).

3.2 Soggetti che accedono ai dati personali nel FSE

Le finalità di cui alla lettera a) sopra richiamate sono perseguite dai soggetti del Servizio sanitario nazionale e dei servizi socio-sanitari regionali e da tutti gli esercenti le professioni sanitarie che prendono in cura l'assistito secondo le modalità di accesso da parte di ciascuno dei predetti soggetti e da parte degli esercenti le professioni sanitarie.

Nel progetto per cui si procede è prevista l'interazione del FSE professionisti, già operativo per gli esercenti le professioni sanitarie, con il portale SAR.

L'interazione del farmacista con il FSE è da considerarsi legittima ai sensi del citato art. 12 del D.lgs. 179/2012, poiché soggetto esercente la professione sanitaria.

Invero, la figura del farmacista rientra certamente nel perimetro soggettivo di cui al citato art. 12, ai sensi e per gli effetti degli artt. 99 e ss. del Regio Decreto n. 1265/1934, nonché del D.lgs. n. 258/1991. L'attività di farmacista, come prevista dall'art. 8, comma 2, del D.lgs. n. 502/1992, è manifestamente riconducibile alla finalità di cura (rectius, ad un segmento della finalità di cura).

In sintesi, il quadro normativo sopra delineato costituisce base giuridica legittimante i trattamenti di dati personali effettuati dai farmacisti per finalità di cura, limitatamente all'accesso alle prescrizioni mediche effettuate dai medici prescrittori.

3.3 Il consenso alla consultazione del farmacista

Per quanto concerne il consenso, l'art. 12, comma 5, del D.lgs. 179/2012 dispone che *"la consultazione dei dati e documenti presenti nel FSE di cui al comma 1, per le finalità di cui alla lettera a) del comma 2, può essere realizzata soltanto con il consenso dell'assistito e sempre nel rispetto del segreto professionale, salvo i*

casi di emergenza sanitaria secondo modalità individuate a riguardo. Il mancato consenso non pregiudica il diritto all'erogazione della prestazione sanitaria".

Tali disposizioni devono intendersi quale parametro minimo di riferimento nella regolamentazione del consenso nel modello che si propone di implementare.

Pertanto, ai fini dell'accesso ai dati e alle informazioni sopra emarginate, il farmacista, qualora non sia stato già rilasciato il consenso alla consultazione del FSE, è onerato di recepirlo dall'Assistito e di tale consenso il sistema tiene traccia nelle modalità sopra indicate, e quindi con i dati del CF dell'assistito, del CF del farmacista che recepisce il consenso, farmacia di afferenza del farmacista, data e ora.

Le Farmacie somministrano agli Assistiti l'informativa per il trattamento dei dati personali ex art. 13 del Regolamento UE 2016/679, utilizzando un modello definito e condiviso con la Regione Emilia-Romagna a cui viene data diffusione anche a mezzo dei siti istituzionali dell'Ente. La piattaforma consente di produrre analisi degli accessi ai dati e alle informazioni di cui sopra da parte dei farmacisti; a titolo esemplificativo, sono sottoposti a controllo logico accesso ai dati e correlata erogazione del farmaco, al fine di rilevare eventuali accessi anomali/abusivi.

4. Misure di sicurezza

Tra i requisiti per la implementazione del nuovo trattamento vi è la

- Richiesta/presenza del consenso dell'assistito
- Identificazione del singolo operatore che ha effettuato l'accesso
- Tracciatura degli accessi alle prescrizioni
- Autenticazione al SAR
- Codice farmacia
- Password
- Pincode

Sono attori nel flusso:

- SAR (Servizio di Accoglienza Regionale) (LEPIDA)
- Portale farmacie (LEPIDA)
- Applicativi farmacie (FORNITORI FARMACIE)

Richiamate le misure di sicurezza valorizzate nella valutazione d'impatto per i trattamenti relativi alla gestione dell'infrastruttura del FSE, sono di seguito indicate alcune misure di sicurezza tecnico-organizzative implementate al fine di ridurre il rischio correlato al trattamento dei dati personali di cui si tratta.

Con riferimento alle misure di sicurezza tecniche ed organizzative idonee a garantire la riservatezza, l'integrità e la disponibilità dei dati, si rappresenta quanto segue.

La gestione tecnologica dell'infrastruttura è regionale e operativamente demandata a Lepida Scapa, società in house partecipata dalla Regione Emilia-Romagna.

4.1 La Gestione degli Asset

Tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni sono specificatamente identificati e l'inventario di tali asset è mantenuto aggiornato in apposito sistema di asset inventory. Le regole per il corretto utilizzo degli asset sono identificate e documentate in apposite policy condivise dalla Regione e da Lepida Scpa, ivi compresi gli utenti con privilegi di amministrazione.

4.2 Provisioning e deprovisioning

Sono previste apposite procedure formali per l'assegnazione o la revoca dei diritti di accesso, per le diverse tipologie di utenze e per i diversi sistemi e servizi. Per quel che concerne gli accessi dei farmacisti, è onere della farmacia assicurare che il soggetto che accede sia legittimato all'accesso.

4.3 Riesame e rimozione degli accessi

I diritti di accesso di tutto il personale di Lepida, ivi compresi i collaboratori a qualsiasi titolo, sono riesaminati a mezzo di apposite verifiche di sicurezza, oltre che su specifica segnalazione.

4.4 Sicurezza fisica e ambientale

L'accesso alle sedi della Regione e di Lepida è disciplinato da apposite procedure di controllo degli accessi. In alcuni locali (ove, ad esempio, sono custoditi materiali di proprietà dell'Ente) oltre al controllo degli accessi effettuato dagli addetti della portineria e/o presidiati dagli operatori della società, sono stati attivati ulteriori sistemi antintrusione costituiti da porte di ingresso chiuse a chiave e allarmate.

La sede del datacenter regionale ove insistono i servizi considerati non presenta criticità ambientali ed è sempre presidiata. La tutela del patrimonio informativo dell'Ente e della sua rilevanza strategica è assicurata dal combinato disposto delle misure tecnico-organizzative adottate dall'Ente, come ad esempio il controllo degli accessi operato dagli addetti di portineria, gli allarmi antincendio, dalla vigilanza delle guardie giurate ecc. ecc., di cui la videosorveglianza costituisce elemento imprescindibile.

4.5 Protezione da malware e spam

Le misure relative all'anti-malware e antispam sono definite nell'ambito dei servizi regionali e di Lepida; nello specifico tutti i componenti anti-malware sono gestiti e monitorati da una interfaccia unica con meccanismi di interazione tra i vari componenti.

4.6 Il Backup

L'Ente e la società hanno approntato soluzioni per il backup centralizzato dei sistemi, dei database, dei file server ed in generale delle soluzioni implementate presso i Datacenter regionali.

4.7 Gestione delle vulnerabilità tecniche

Sono monitorati periodicamente i bollettini ricevuti dai Vendor o da Enti come CSIRT e in particolare i bollettini in ambito sicurezza.

4.8 Limitazione alle installazioni software

Gli utenti non dispongono di privilegi amministrativi sulle postazioni di lavoro, quindi non possono installare autonomamente. Le richieste di installazione di nuovo software non in catalogo sono gestite direttamente dalla struttura IT competente.

4.9 Attività di audit

Sono svolti costanti monitoraggi della sicurezza dei sistemi e sono svolti periodici audit, anche in ragione delle certificazioni ISO27001 che sia Lepida che la Giunta regionale hanno ottenuto e mantenuto.

4.10 Sicurezza della rete

Sono attivati meccanismi di monitoraggio della rete. Lepida, che gestisce, altresì, la rete implementa meccanismi di gestione di sicurezza della connettività. In ogni caso, tutti i sistemi, i servizi e le applicazioni esposti sulla rete regionale sono soggetti all'obbligo di autenticazione e permettono l'accesso unicamente agli utenti autorizzati.

4.11 Firewall

La rete regionale è protetta da accessi indesiderati provenienti dalla rete Internet attraverso un sistema firewall complesso.

4.12 Comunicazioni cifrate

Per i flussi descritti nel presente documento sono impiegati meccanismi di cifratura delle comunicazioni, ovvero la trasmissione dei dati avviene su canali cifrati.

4.13 Gestione degli incidenti di sicurezza

La Regione e Lepida hanno adottato policy e procedura per la gestione degli incidenti di sicurezza informatica. La corretta gestione degli incidenti di sicurezza è misura che consente di evitare o di minimizzare la compromissione dei dati dell'organizzazione in caso di incidente; inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, la corretta attuazione di tale policy e procedura consente di migliorare continuamente la capacità di risposta agli incidenti.

4.14 Business Continuity

La Regione e Lepida hanno adottato un Piano di Business continuity che si pone la finalità di garantire la continuità dei servizi IT a fronte di uno scenario di disastro.