Agostino Grignani,
Managing Director
CYSED Srl

La ricetta elettronica nell'emergenza pandemica

Farmacia e paziente in remoto, l'interazione digitale: opportunità e rischi indotti dalla ricetta elettronica e dalla pandemia

Nella fase iniziale della pandemia, nel marzo dello scorso anno, l'ordinanza della Protezione Civile n. 651 del 19 marzo conteneva, fra le varie misure emergenziali, una importante novità per rendere più agevole l'accesso alle prescrizioni di farmaci rimborsati Ssn. In estrema sintesi, l'ordinanza tuttora in vigore, prevedeva all'art.1 che l'assistito potesse richiedere al medico prescrittore di una ricetta elettronica, di effettuare l'invio all'assistito stesso dell'Nre (numero di ricetta elettronica) o del documento di promemoria, tramite un canale digitale: posta elettronica, *Sms* e implicitamente anche via *instant messaging* (WhatsApp, *Telegram*, eccetera). Il principio del provvedimento era quello di evitare, in una fase di *lockdown* e di difficile accesso agli studi medici, problemi nel ritiro dei promemoria delle ricette elettroniche e quindi di approvvigionamento dei farmaci. L'attivazione di un canale di trasmissione digitale di Nre/promemoria dal medico prescrittore era già contemplato nel decreto cardine sulla ricetta elettronica (DM 2/11/2011), ma dopo quasi dieci anni non aveva ancora avuto attuazione concreta e omogenea in tutte le Regioni. **Il problema della trasmissione per canale digitale al posto della consegna fisica del promemoria è stato dibattuto in tutti questi anni, ma solo la pandemia ha portato in pochi giorni a un'immediata e pragmatica applicazione. Certo, il problema dell'emissione di una prescrizione di un farmaco in remoto è argomento delicato, d'altra parte molte delle prescrizioni di farmaci sono ripetute per patologie croniche, che non necessitano una visita di persona del paziente**. L'evoluzione, anche normativa, della telemedicina darà alla tele-visita lo stesso valore della visita in presenza. Ma se il paziente con l'ordinanza del marzo 2020 poteva ricevere digitalmente Nre/promemoria dal medico, poteva anche trasmetterlo digitalmente alla farmacia? Questo aspetto, non chiarito dal testo dell'ordinanza, sebbene implicitamente desumibile, è stato meglio definito da un successivo decreto:

il DM MEF/SALUTE del 30/1/2021. Il nuovo DM, riguardante la ricetta elettronica per le prescrizioni non rimborsabili di farmaci, sebbene non ancora implementato in concreto, **regola la trasmissione digitale del promemoria/Nre dall'assistito alla farmacia con modalità differenti tra l'attuale fase emergenziale pandemica e quella a regime**. Nella fase emergenziale l'assistito potrà inviare Nre/promemoria, ricevuto digitalmente dal prescrittore (o anche scaricato nel proprio Fse), alla farmacia sempre per gli stessi canali digitali di posta elettronica, *Sms* e *instant messaging*, come in ricezione dal medico. **Nella fase a regime la trasmissione digitale diretta alla farmacia avverrebbe con una nuova modalità: il paziente potrà infatti collegarsi al sito della Tessera sanitaria indicando una farmacia di riferimento a cui verranno inviati gli Nre/promemoria**. Lo scenario a regime del portale Tessera Sanitaria sembra ancora molto lontano, limitiamoci quindi a valutare il modello di questa fase di emergenza che si può ritenere valga anche per le ricette elettroniche dei farmaci rimborsabili.

PAZIENTE E COMUNICAZIONE DIGITALE CON LA FARMACIA

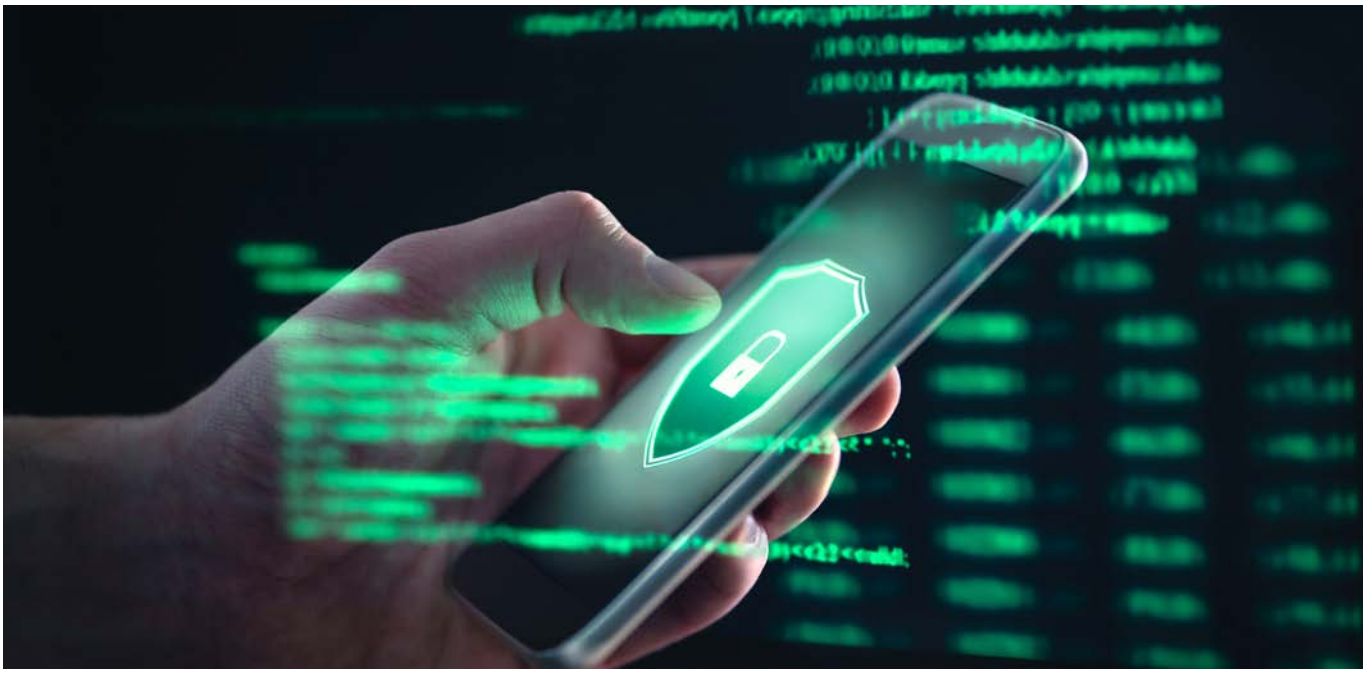
Cerchiamo prima di capire, limitatamente alla ricetta elettronica, se questa comunicazione digitale paziente-farmacia sia effettivamente decollata. Per rispondere a questa domanda dobbiamo anteporne un'altra: gli assistiti hanno attivato la trasmissione digitale di Nre/promemoria dal loro medico prescrittore? Sembra proprio che lo abbiamo fatto, anche dopo la fase di *lockdown* stretto; una ricerca di Doxa Pharma condotta nel novembre 2020 ha infatti rilevato che il 92 per cento dei rispondenti aveva sperimentato senza difficoltà la trasmissione digitale di Nre/promemoria dal prescrittore (*https://www.bva-doxa.com/next-generation-health-le-priorita-degli-italiani-per-la-sanita-del-futuro/*).
Veniamo però al punto: quanti hanno poi trasmesso Nre/promemoria per via digitale all'indirizzo *e-mail* della farmacia o per *Sms*/Im a un suo numero di telefono? Non disponiamo in questo caso di numeri precisi, la sensazione che però si evince è che buona parte degli assistiti si siano presentati direttamente

©Syda Productions\shutterstock.com

in farmacia esibendo Nre/promemoria dal proprio cellulare. Chi ha inviato in anticipo per *e-mail* o WhatsApp alla farmacia sembra essere una minoranza, lo stesso dicasi per una serie di *app* volte proprio a favorire questa comunicazione in un ambiente sicuro e facilitato, si veda per esempio *https://ricettainfarmacia.it*. Un altro fenomeno presente ma, con incidenza limitata e forti dubbi di legittimità ha sicuramente riguardato la trasmissione diretta, su indicazione dell'assistito, di Nre/promemoria dal prescrittore alla farmacia. **La situazione è evidentemente ancora ingarbugliata** con **un nuovo modello di comunicazione digitale in arrivo, attraverso la scelta della farmacia di riferimento sulla piattaforma della Tessera Sanitaria**. Comunque sia, è evidente che sui vari fronti indotti dalla pandemia, come ricetta elettronica, consegne a domicilio, tamponi e vaccinazioni in farmacia, la comunicazione digitale diretta paziente-farmacia è destinata ad aumentare. Nel solo ambito delle consegne a domicilio dei farmaci si contano già una decina di *app* attive. **Occorre perciò che la farmacia non solo migliori l'efficacia della propria comunicazione digitale, ma anche che la sviluppi con la giusta consapevolezza sui rischi per la sicurezza informatica**. Passare dal non ricevere *e-mail* a un traffico giornaliero importante obbliga la farmacia a una revisione dei propri processi informatici, nonché a un adeguamento dei comportamenti più adatti alla comunicazione digitale. Per molti aspetti la farmacia che aderisce a un'*app* per comunicare con i suoi pazienti aumenta sicuramente il proprio profilo di sicurezza informatica.

COS'È IL PHISHING

L'incremento del traffico di *e-mail* da contatti non già noti espone al rischio di cadere nel *phishing*. I messaggi di ***phishing*** consistono in *e-mail* fraudolente, che in alcuni casi contengono un ***link*** simile alla schermata di accesso a un servizio: la vittima inserendo le proprie **credenziali** crede di **accedere** al sito originale, invece invia le stesse a chi ha creato il sito fasullo. In altri casi nella *e-mail* è contenuto **un allegato malevolo: un *malware*, che può tracciare e bloccare le attività che si svolgono sul *computer*, o rubare le credenziali di accesso, o distruggere i *file* contenuti in esso**. Ultimamente i criminali utilizzano anche **altri canali** per gettare le loro esche, oltre all'*e-mail*: Whatsapp, Facebook o Linkedin, ma il procedimento è sempre lo stesso.



© Tero Vesalainen\shutterstock.com

Generalmente questi messaggi vengono creati in modo che sembrino originati da:

- servizi che hanno accesso a una **carta di credito**: banche, Amazon, e-Bay;
- servizi che hanno accesso a **informazioni personali**: Facebook, Instagram, Linkedin;
- servizi di *storage cloud*, che contengono **documenti**: iCloud, Drive, Dropbox;
- **autorità**: uffici legali, polizia postale, il direttore / reparto IT della nostra azienda;
- colleghi di lavoro o **persone che conosciamo** (*spoofing*).

Nelle mail di *phishing* l'attaccante spesso cerca di far leva sulle **emozioni del destinatario** oppure di approfittare di un momento di **disattenzione** dello stesso: si tratta di tecniche di ***social engineering***. Talvolta hanno carattere di urgenza e richiedono **un'azione immediata**: un *click* a un *link* o il *download* di un allegato. La **paura** delle conseguenze del mancato intervento, indotta dall'attaccante al destinatario, serve a generare una risposta veloce e poco ragionata, che crea una porta di accesso per il *phisher*.

Vediamo alcuni esempi di *e-mail* che inducono un senso di **allerta**, di **urgenza**:

- «il tuo *account* *** verrà temporaneamente chiuso perché inutilizzato, se vuoi mantenere attivo il tuo *account* aggiorna le tue informazioni al seguente *link*»;
- «è stata rilevata un'attività sospetta: tentativo di accesso al suo *account* ***, se non sei stato tu a eseguire questa attività è necessario cambiare la *password* dell'*account* al seguente *link*»;
- «mancata consegna del pacco numero ***, in allegato le istruzioni per contattare il corriere».

In altri casi si tratta di **offerte allettanti** come proposte di lavoro, *download* di *coupon* contenenti sconti per hotel, un messaggio di un amico (*hackerato*) in difficoltà che chiede un favore.

QUALCHE RACCOMANDAZIONE

Un attacco di *phishing* può avere **effetti devastanti** sulla farmacia, soprattutto se l'attacco mira al blocco di tutte le attività informatiche gestite dalla farmacia: ricetta dematerializzata dei farmaci e dei prodotti veterinari, ordini *on line*, servizi Cup, eccetera. Anche nel caso di *data breach* di dati personali degli assistiti, detenuti negli archivi della farmacia, le conseguenze sono molte negative con il rischio di una notifica al garante della *privacy*. Poiché l'attacco di *phishing* sfrutta la vulnerabilità psicologica dell'utente finale, il farmacista deve essere sensibilizzato sul tema e formato per riconoscere gli elementi che caratterizzano una *e-mail* malevola. Indubbiamente *firewall*, *antivirus* e *antispam*, creano un primo livello di protezione; in tale contesto sono determinanti le decisioni della farmacia in merito a quali strumenti adottare e a quali *app* di comunicazione digitale appoggiarsi. Nei casi però, molto frequenti, dove l'indirizzo *e-mail* della farmacia coincide con quello personale del farmacista, le protezioni tecniche potrebbero essere deboli; in questi contesti la consapevolezza del farmacista sui rischi informatici è fondamentale. La commistione di uso personale e uso per la farmacia soprattutto attraverso lo *smartphone* del farmacista è una delle aree di maggiore vulnerabilità. È possibile inoltre effettuare errori di invio di informazioni o documenti sensibili, un invio al mittente sbagliato potrebbe comportare un grosso rischio per la *privacy* del cliente. La minaccia di *phishing* si sta spostando velocemente anche su canali come *Sms* e Whatsapp, strumenti sempre collegati all'utilizzo dello *smartphone*. La conoscenza dei rischi e degli strumenti digitali da parte dei farmacisti è alla base della sicurezza dei dati che vengono trattati e della continuità del servizio offerto ai clienti e ai pazienti. ●

© Svetlana Sotnikova\shutterstock.com