PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5249 di Mercoledì 05 ottobre 2022

I rischi della telemedicina: un contributo al convegno nazionale

Da più parti si afferma che una delle possibili soluzioni al problema dell'affollamento ospedaliero è legato a una crescente diffusione della telemedicina. L'affermazione è accettabile, ma fino a un certo punto.

Il prossimo 11 e 12 Ottobre 2022 presso l'Aula Magna del Centro di Biotecnologie della Università degli Studi di Napoli "Federico " si terrà la XIX edizione del Convegno Nazionale Ospedale Sicuro Duemila22, organizzato e promosso dall'Osservatorio Salute Lavoro del Dipartimento di Sanità Pubblica.

Si tratta di un convegno di grande rilievo, perché non v'è dubbio che il problema della sicurezza, in un contesto ospedaliero, assume un ruolo sempre più significativo.

Non per nulla, alcune strutture ospedaliere già da tempo hanno designato un dirigente, come responsabile della security, proprio per dotarsi di una figura di riferimento su un tema, che talvolta passa in secondo piano, rispetto all'obiettivo primario della struttura ospedaliera, che è quello di consentire ad un paziente di recuperare appieno la sua salute.

Questo tema è assai caro all'autore di questo articolo, che già tempo fa, in collaborazione con un responsabile della sicurezza di una struttura ospedaliera, pubblicò un volume specialmente dedicato alle caratteristiche di un "ospedale sicuro".

Con l'aumento delle prestazioni di telemedicina, occorre prestare la massima attenzione al fatto che tali prestazioni avvengano in un contesto sufficientemente affidabile, non tanto sul piano sanitario, che non è problema di chi scrive, ma sul piano della sicurezza e affidabilità di tutto ciò che è connesso alla telemedicina.

Tanto per cominciare, i pazienti potrebbero non essere consci del fatto che le informazioni riservate, afferenti alla loro salute, potrebbero essere ascoltate o rivelate, in modo inappropriato, durante un collegamento video.

Ecco alcune raccomandazioni su come è possibile mettere sotto controllo questo rischio.

- Tanto per cominciare, il responsabile del servizio informativo ospedaliero dovrebbe sviluppare un programma, che permetta di tenere sotto controllo tutti i collegamenti audiovideo, effettuati dai pazienti, a distanza. Sarà così possibile evidenziare potenziali situazioni di rischio, che potranno essere tempestivamente messe sotto controllo.
- Il responsabile del servizio informativo ospedaliero dovrebbe sensibilizzare i pazienti, assistiti a distanza, sulle appropriate tecniche di protezione del collegamento, durante il quale potrebbero essere scambiati dati personali di rilevanza sanitaria. Questa informazione sulla protezione del collegamento deve essere espressa in termini facilmente comprensibili, anche a persone che non sono dotate di specifica cultura informatica.

- Nel limite del possibile, e compatibilmente con gli apparati disponibili presso il paziente, la adozione di collegamenti cifrati permette di elevare in maniera significativa il livello di protezione dei dati scambiati, sia video, sia audio, tra il paziente e la struttura ospedaliera.
- Per quanto possibile, è opportuno che il dispositivo utilizzato per il collegamento di telemedicina, sia audio, sia video, venga utilizzato in esclusiva dal paziente e non sia condiviso con altri soggetti, che potrebbero avere l'opportunità di accedere a dati, deliberatamente o accidentalmente registrati sul dispositivo.

Queste raccomandazioni vengono riassunte in uno studio, condotto dal General accounting Office, negli Stati Uniti, che ha analizzato tutte le segnalazioni afferenti a servizi di tele sanità, gestiti dal servizio Medicare, dal 2019 fino al 2020.

Adalberto Biasiotti

---

www.puntosicuro.it