

Telemedicina e Privacy - l'eterna lotta tra i due mondi in cui anche l'Italia dice la sua

LINK: <http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2017-07-04/telemedicina-e-privacy--eterna-lotta-i-due-mondi-cui-anche-italia-dice-sua...>



Telemedicina e Privacy -l'eterna lotta tra i due mondi in cui anche l'Italia dice la sua Avv.ti Riccardo Sciaudone ed Eleonora Caravà dello studio **R&P Legal** | 04/07/2017 10:34 Tweet My24 Aumenta dimensione font Diminuisci dimensione font Stampa l'articolo Invia articolo per email Introduzione

Nell'ambito del Programma europeo Horizon 2020 (<https://ec.europa.eu/programmes/horizon2020/>), ideato per finanziare progetti di ricerca ed innovazione, il progetto ReMeDi - Remote Medical Diagnostician (http://cordis.europa.eu/project/rcn/110646_en.html), coordinato dall'Università West of England, ha creato e sviluppato un prototipo di robot "dottore" che consente al personale medico di visitare i pazienti anche in caso di grandi distanze. Tra i vari Stati membri coinvolti in questo progetto "multijurisdictional" (vale a dire, progetto in cui partecipano - e beneficiano dei fondi Ue - più Stati membri), c'è anche la Scuola Superiore Sant'Anna di Pisa che, insieme ad altre prestigiose università di Austria, Svizzera, Polonia e Germania, ha raggiunto un livello ulteriore e successivo nel processo di diffusione e penetrazione capillare della telediagnostica nel settore sanitario. Tema, questo, che solleva però tanti interrogativi dal punto di vista della tutela dei dati personali. I prodigi del robot "dottore" che sollevano criticità privacy Il prototipo multifunzionale, attualmente situato in un ospedale polacco, ma che, per "farsi conoscere", sta facendo il giro del mondo, consente al personale medico di intervenire anche a distanza nella diagnosi del paziente o di chiedere una consulenza ad un medico specialista che non si trova fisicamente nella stessa stanza del paziente. Nella consapevolezza che un trattamento medico efficace dipende non soltanto da diagnosi tempestive e corrette, ma anche dalla disponibilità di medici specializzati e competenti, la quale, in alcuni contesti, è piuttosto limitata (ad esempio, nei Paesi che soffrono di penuria di personale qualificato o in cui è difficile l'accesso all'assistenza medica specializzata), l'obiettivo perseguito con il progetto ReMeDi è stato quello di mettere a disposizione uno strumento di diagnosi in remoto che consentisse una collaborazione "in remoto" tra professionisti del settore di diverse strutture sanitarie e, in alcuni casi, di diversi Paesi. Il robot "dottore" è in grado di tradurre i comandi del medico in input tattili aventi diverse intensità di forza, è dotato di sensori che percepiscono il grado di umidità e la temperatura corporea del paziente e riesce a carpire tutta una serie di informazioni ulteriori che, di norma, i medici captano, ad esempio, solo con la palpazione del corpo umano. Il robot "performa" un reale esame fisico e ultrasonografico e ciò è possibile in ragione della particolare superficie di cui esso è dotato il robot e di un dispositivo "tattile" ivi incorporato (dispositivo che ha una superficie soffice che ricorda la pelle e che è in grado di replicare il tatto umano). Tra le innumerevoli e interessanti applicazioni, tale prototipo comunica al medico la rigidità addominale del paziente, nonostante il medico sia seduto a centinaia di chilometri di distanza e guardi il paziente davanti a tre monitor. La protezione dei dati personali nella telemedicina: problemi e consigli pratici La telemedicina, ormai fenomeno emergente, garantisce innumerevoli benefici per le strutture sanitarie e i medici, che possono agevolmente comunicare a distanza con i propri colleghi e aumentare la propria expertise. Ma anche i pazienti - specialmente quelli che soffrono di patologie croniche - possono goderne, ad esempio nel caso di consulti a distanza. Tuttavia, le strutture sanitarie che

desiderino dare ampia diffusione a questo strumento necessitano, per poter erogare servizi sanitari di telemedicina, di informazioni relative allo stato di salute del paziente. Da qui, alcune delle domande sorgono in relazione a come tutelare i dati sanitari dei pazienti, anche e soprattutto in ragione della nuova disciplina in materia di tutela della protezione dei dati personali introdotta dal Regolamento Ue 2016/679, e cioè il regolamento generale sulla protezione dei dati (il "Regolamento"). L'attenzione è, innanzitutto, allertata in caso di scambio di dati sanitari del paziente tra Stati membri e tra Stati Ue e non-Ue, scambio che rappresenta il cuore della telemedicina e dell'erogazione dei servizi sanitari a distanza. Se i dati sanitari sono trasferiti fuori dallo Spazio economico europeo (quindi in Paesi dove il Regolamento non è applicabile), dovrebbero esser prese in considerazione restrizioni ulteriori, magari anche di natura contrattuale (si vedano, ad esempio, gli accordi USA-Ue per gli scambi transfrontalieri). Il soggetto che trasmette i dati dovrebbe, come prima cosa, valutare se il Paese in cui vuole trasferire i dati del paziente assicura un grado di protezione lato privacy adeguato. Tale valutazione deve basarsi sicuramente sulle circostanze del caso concreto, ma non può prescindere dall'esame delle finalità del trattamento, dei motivi che giustificano il trasferimento dei dati, della sua durata e delle misure di sicurezza che, come minimo, devono essere assicurate. Altro elemento fondamentale è l'analisi del "rischio paese", vale a dire, l'esame dei rischi in cui un operatore incorre andando a trasferire i dati sanitari dei propri pazienti in un altro Stato, di cui non conosce appieno le leggi in materia privacy. Ad esempio, alcuni trasferimenti di dati sanitari dovrebbero presupporre la sottoscrizione di specifici contratti tra il soggetto che opera in Europa e quello che invece è stabilito in un Paese non-Ue oppure imporre la firma di protocolli di intesa o l'adesione a policy aziendali o linee guida più stringenti. Sebbene questa sia una valutazione da effettuare con particolare cura nel caso di trasferimenti tra diversi Stati, detta analisi deve esser effettuata - con la medesima attenzione - anche nel caso in cui il titolare voglia trasferire i dati sanitari ad altro soggetto o struttura sanitaria del suo stesso Paese (ad esempio, scambio di dati tra due ospedali italiani). Anche in questo caso il titolare che trasferisce i dati deve assicurarsi che chi li riceve abbia un livello di competenze adeguato a garantire la protezione delle informazioni scambiate e ad implementare misure di sicurezza idonee. Elemento imprescindibile in qualsiasi trasferimento di dati, soprattutto se sanitari (in quanto appartenenti alla categoria dei dati sensibili soggetti a maggior tutela), è la corretta informazione che si dà al paziente e l'ottenimento di un suo consenso al trasferimento, specie se transfrontaliero. Quello che si consiglia ai titolari del trattamento che siano decisi ad erogare servizi di telemedicina è, infatti, la creazione di policy aziendali e di procedure di raccolta del consenso del paziente che siano in linea non solo con gli standard legali nazionali, ma che siano soprattutto accettabili negli ordinamenti giuridici degli altri Paesi (o almeno di quelli con cui si vuole fare telemedicina transfrontaliera). Un altro problema privacy che viene sperimentato con la telemedicina riguarda il frequente uso di database cloud che servono per conservare i dati sanitari necessari per le prestazioni di telemedicina, in ragione del fatto che una conservazione oltre un certo periodo (quello necessario per la prestazione) denota un mancata conformità ai dettami del nuovo Regolamento. Un'ulteriore criticità si ha se si considera che la disciplina privacy, specie con il Regolamento, impone un divieto acchè i dati sanitari siano trattati da soggetti diversi da quelli esercenti la professione sanitaria e siano soggetti al segreto professionale. Il problema sorge perché la telemedicina, di norma, coinvolge anche soggetti diversi dal personale sanitario, come i reparti IT. Per risolvere questo problema, si consiglia ai titolari di far firmare al personale IT degli accordi di riservatezza e confidenzialità, aventi forma e valore di impegno contrattuale, oltre che nominarli incaricati del trattamento.