LE GUIDE DI CONSULCESI CLUB

DIRITTI E OBBLIGHI LEGALI DEI MEDICI SUL WEB: UNA GUIDA COMPLETA

CONSULCESI CLUB

INDICE

La vita di ognuno di noi si svolge, volente o nolente, su due dimensioni parallele: online e offline. La vita online è soggetta al rispetto delle regole del web (ad esempio le condizioni di utilizzo di una piattaforma social), delle norme giuridiche e delle regole di buona educazione che dovrebbero caratterizzare i comportamenti di ognuno di noi in ogni contesto.

Così come nella vita reale un professionista non smette mai di essere tale, lo stesso accade per la proiezione online di quel determinato soggetto, sia esso un avvocato, un commercialista, un architetto o un medico. In particolare, nel complesso contesto del settore medico, è importante che il professionista della salute sia consapevole delle regole da seguire per navigare sul web in tutta sicurezza, senza incorrere in comportamenti professionalmente o deontologicamente scorretti o – peggio ancora – antigiuridici, proteggendosi così da eventuali rischi legali.

1. LA LIBERTÀ DI ESPRESSIONE DEL MEDICO E I SUOI LIMITI

La libertà d'espressione è uno più importanti diritti fondamentali dell'uomo: si ha democrazia quando i cittadini possono esprimersi liberamente, senza censure e nel rispetto reciproco. La libertà di espressione, oltre che dall'articolo 21 della Costituzione italiana, è garantita a livello europeo dalla Carta dei diritti fondamentali dell'Unione, che include, all'interno di questa fondamentale libertà, quella di esprimere liberamente la propria opinione, di ricevere o comunicare informazioni o idee senza che vi sia alcun tipo di ingerenza da parte delle autorità pubbliche e senza limiti di frontiera.

Il medico, in quanto cittadino, gode del diritto alla libera manifestazione del proprio pensiero, ed è libero di pubblicare su un sito web o sui propri profili social le sue opinioni, purché – in un'ottica di bilanciamento tra diritti e doveri – **lo faccia senza travalicare mai il suo ruolo di professionista al servizio della tutela della vita, della salute fisica e psichica dell'uomo, nel rispetto della libertà e della dignità della persona umana, senza discriminazioni di età, sesso, razza, religione, nazionalità, condizione sociale, ideologia**.

In virtù di questi principi, ad esempio, un professionista sanitario non può diffondere su chat di messaggistica istantanea fotografie che lo raffigurino con pazienti deceduti, pena la radiazione: una condotta del genere, indipendentemente dalla divulgazione o meno delle immagini, rivela un atteggiamento di spregio della vita umana ingiustificabile, che non trova attenuante nemmeno in particolari condizioni, stati d'animo o psicologici che possano in qualche modo aver indotto il sanitario anche soltanto a concepire – e poi a realizzare – un comportamento così inutile e spregevole.

Ulteriore esempio di **bilanciamento tra libertà di manifestazione del pensiero e principi deontologici** si è avuto nel corso della pandemia, che ci ha dimostrato quanto l'opinione qualificata di un professionista sanitario possa influenzare – in positivo o in negativo – le persone spaventate per la loro salute. Per contemperare la libertà di manifestazione del pensiero e l'obbligo gravante sul sanitario di tutelare la salute umana, numerosi professionisti del settore che hanno negato l'esistenza del Covid sulle proprie pagine social, contribuendo così a diffondere vere e proprie ***fake news***, sono stati sottoposti a **sanzione disciplinare** per aver **depistato, confuso e disinformato i pazienti**.

L'**autocelebrazione** esagerata e ingiustificata della propria professionalità, attraverso l'utilizzo sul proprio sito web o sui social di **frasi comparative e non sostenute da dati scientifici** del tipo "l'unico medico a eseguire la prestazione xxx in meno di un'ora su tutto il territorio nazionale", rappresenta un ulteriore esempio di come la libertà di manifestazione del pensiero del professionista sanitario debba arrestarsi di fronte al rischio di fuorviare i pazienti e di allontanarsi dal dovere di tutelare la vita e la salute dell'uomo.

2. LA LIBERTÀ D'ESPRESSIONE DEL MEDICO SUI SOCIAL NETWORK

Sui *social network* non è consentito pubblicare qualunque tipo di opinione, foto, video o post. In generale, le piattaforme bannano i contenuti violenti, che incitano all'odio, allo sfruttamento sessuale minorile, che incitino le persone ad abusi o molestie o al suicidio. Le condizioni di utilizzo di piattaforme come Meta o X (il vecchio Twitter) bandiscono inoltre l'utilizzo dei loro servizi per scopi illegali o per promuovere attività illegali, per pubblicare dati inerenti la privacy di terzi senza il loro consenso (ad esempio il numero di cellulare o l'indirizzo di una persona) e per attuare condotte riprovevoli come la pubblicazione di video/foto di nudo non consensuale di adulti o minori.

Meta, in particolare, garantisce agli utenti di impegnarsi per perseguire la libertà di espressione della *community* che lo utilizza, e per evitare usi impropri di internet limita questa libertà solo per tutelare i seguenti valori:

autenticità • la Società vuole assicurarsi che le persone vedano solo contenuti autentici, in modo da creare un ambiente migliore per la condivisione,

sicurezza • la Società rimuove i contenuti che potrebbero contribuire a un rischio di violenza per la sicurezza fisica delle persone, i contenuti che comportano minacce per le persone o che possano intimidire, escludere o mettere a tacere gli altri,

privacy • la piattaforma protegge le informazioni e la privacy, impegnandosi a garantire ai suoi utenti di scegliere come e quando condividere,

dignità • i contenuti devono garantire il rispetto della dignità delle persone, perciò di base vengono bannati i post/foto/video che non rispettino la dignità altrui o che minaccino o denigrino il prossimo.

In realtà, facendo *scrolling* sulle piattaforme Meta o su qualunque altro tipo di piattaforma, notiamo che è davvero difficile per queste Società arginare il fenomeno generale dell'odio online, soprattutto nei commenti ai post, come di recente accaduto sui post collegati alla famiglia Ferragni dopo la vicenda del pandoro-*gate*.

Al di là di questi fenomeni limite, comunque, il professionista sanitario che decida di utilizzare una piattaforma social, oltre che alle regole del buon senso e alle norme deontologiche, deve rispettare anche e soprattutto le condizioni di utilizzo della singola piattaforma e le regole della *community*, che si possono consultare dalle Homepage di qualunque piattaforma.

2.1 LE RACCOMANDAZIONI DELLA FNOMCEO SULL'USO DEI SOCIAL DA PARTE DEI MEDICI

L'uso personale e professionale dei social media da parte dei professionisti della salute è inevitabile ed è in costante crescita; gli anni della pandemia, con le persone forzatamente a casa davanti agli schermi, hanno generato nuovi fenomeni comunicativi in ogni settore, compreso quello della salute. La divulgazione di informazioni e notizie mediche *user friendly* sui social e l'accorciarsi della distanza comunicativa tra medico e paziente – che oggi *chattano* su qualunque piattaforma discutendo di patologie, diagnosi e cura – sono fenomeni comunicativi imponenti, che mai avremmo immaginato potessero far parte delle nostre vite prima del Covid.

Per questo il Gruppo di Lavoro ICT della FNOMCeO nell'estate 2023 ha elaborato un documento con alcuni suggerimenti e raccomandazioni che possano aiutare il medico, in assenza di una regolamentazione specifica, a capire cosa può e cosa non può fare sul web e quali accorgimento adottare per evitare di compiere azioni contrarie alla legge o al Codice deontologico.

La FNOMCeO suggerisce ai medici che vogliano utilizzare i *social media* di **aprire due distinti account**, uno **personale** e uno **professionale**. Il profilo professionale deve essere **epurato da qualunque dato sensibile** che possa ricondurre in qualche modo ai pazienti (anche una semplice foto della sala d'attesa dello studio), e dovrebbe contenere solo informazioni generali sulla salute e la pratica clinica, l'informazione scientifica e i link ad altri siti web scientifici (la cui veridicità delle informazioni sia previamente verificata dal medico).

È **sconsigliabile addentrarsi in discussioni professionali con altri colleghi** su *social media* "generalisti" come Facebook, X (il vecchio Twitter), TikTok, Instagram, per evitare che i pazienti siano confusi da discorsi tecnici per loro poco comprensibili e possano avere accesso a informazioni mediche inadatte al loro caso specifico; meglio preferire i *social network* professionali come LinkedIn oppure le *community online* frequentate esclusivamente da medici, come i classici forum all'interno dei quali si accede registrandosi con una username e una password.

La FNOMCeO raccomanda ai medici, nel presenziare sui *social network*, la massima attenzione sulla **riservatezza dei dati**, e a tal fine precisa che il medico è obbligato a non divulgare, in assenza di un consenso appropriato, i dati del paziente, anche sui *social media* e, in generale, sul web. Quando il medico scrive un post, ad esempio, su un caso che gli è capitato, deve fare in modo di privarlo di tutti i dati che potrebbero consentire al paziente di riconoscersi: fin quando le informazioni e i post sono anonimizzati, il medico non corre alcun rischio, mentre in caso contrario potrebbe esporsi a richieste risarcitorie, a segnalazioni al Garante Privacy e all'Ordine di appartenenza per violazione del segreto professionale.

Quando, ad esempio, il biologo nutrizionista pubblica le foto di un suo paziente PRIMA e DOPO il trattamento, indicando con dovizia di particolari i kg e i cm persi e la durata del trattamento nutrizionale, deve munirsi di apposito **consenso per divulgare l'immagine del paziente**, che lo identifica e lo riconduce alla cura medica cui si è sottoposto; in mancanza di consenso, la caccia di like o la semplice voglia di fare una pubblicità un po' fai da te sul web rischia di costare molto cara al professionista sanitario.

In molti, su questo tipo di profilo social, tentano di aggirare il problema del consenso pubblicando foto dei pazienti PRIMA e DOPO il trattamento con la parte della testa tagliata, in modo da rendere irriconoscibili le persone: è consigliabile però, anche in questi casi, munirsi di apposito consenso scritto, quantomeno per non minare il **rapporto fiduciario** tra medico e paziente, che riconoscendosi nudo sul profilo del suo medico senza avergli dato il permesso potrebbe avere più di qualcosa da ridire, in termini morali e legali.

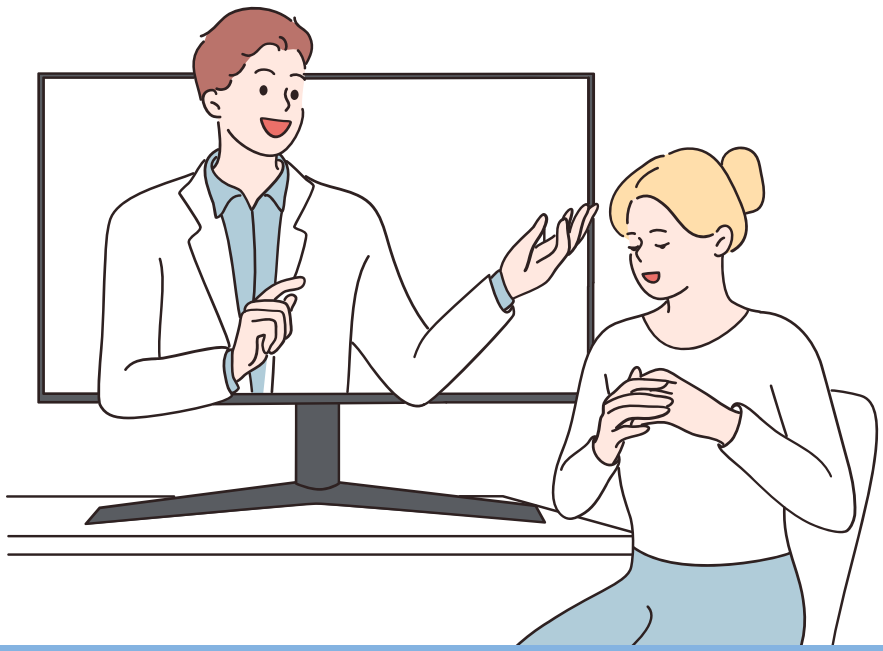
2.2 L'AMICIZIA VIRTUALE MEDICO-PAZIENTE

Il rapporto tra il medico e il cittadino, quale suo potenziale paziente, è fondato sulla reciproca fiducia, sulla libertà di scelta, sull'individuazione e condivisione delle rispettive autonomie e responsabilità, sul rispetto dei valori e dei diritti e su un'informazione comprensibile e completa.

Lo smartphone ha reso estremamente facile, per chiunque, accedere a un social network, azzerando sempre più le barriere e le inibizioni delle persone; il rischio, per il professionista medico, è di una malsana commistione tra vita personale e vita professionale.

L'aumento di confidenza tra medico e paziente, l'utilizzo di un linguaggio familiare e l'accesso, per il paziente, a informazioni personali del suo medico rischia di aumentare il pericolo di transfert del paziente verso il suo medico.

La raccomandazione della FNOMCeO è quella di evitare di accettare richieste di amicizia dai propri pazienti sulle varie piattaforme social. In Gran Bretagna la *British Medical Association* suggerisce ai medici il vero e proprio rifiuto delle richieste di amicizia di pazienti, ritenendo i ***social media*** **un canale inappropriato per ogni interazione medico-paziente**.



2.3 LA PRESENZA ONLINE E I CONFLITTI DI INTERESSE

Se un medico, con il suo profilo professionale, riesce ad avere tanti *follower* – cioè le persone che lo seguono – è inevitabile che venga contattato da aziende che gli chiedono di sponsorizzare, anche velatamente, i propri prodotti dietro compenso. Si tratta di una pratica scorretta sia *online* che *offline*, contraria a ogni principio etico cui un medico dovrebbe attenersi.

Per evitare ogni equivoco, il professionista deve evidenziare, nei suoi post sui social, l'esistenza di eventuali conflitti di interesse, proprio come avviene nella realtà quando si effettua una relazione scientifica presso enti pubblici o privati o in occasioni di congressi e simposi. La FNOMCeO suggerisce di esplicitare il conflitto di interesse con un "*tag*" oppure utilizzando l'hashtag **#noCOI** per indicare l'assenza di conflitto di interesse e **#COI** per segnalarne la presenza, anche se, facendo una breve ricerca sui social e sui principali motori di ricerca, in realtà, non troviamo proprio traccia dell'utilizzo di questi hashtag, che sembrano sconosciuti al web nonostante le raccomandazioni della FNOMCeO.

2.4 LA REGOLA DEL BUON SENSO

In generale, quando un professionista sanitario naviga sul web o utilizza i *social network* e decide di esprimere la propria opinione *online*, deve sempre utilizzare la regola del **buon senso**. Il filtro di uno schermo e di una tastiera non può e non deve rappresentare una maschera dietro cui nascondersi per esprimere opinioni e compiere atti che, dal vivo, non ci sogneremmo mai di attuare. Il professionista sanitario, *online* così come *offline*, deve tenere una **condotta consona a quello che è il suo ruolo e il suo giuramento**, agendo e parlando senza mai dimenticare di avere un compito importante, che è quello di **tutelare la vita e la salute dell'essere umano**.

Internet never forget, e un contenuto postato *online* senza riflettere può diventare virale e incontrollabile in men che non si dica, rischiando di compromettere irrimediabilmente la carriera – oltre che la vita privata – di un professionista sanitario.

3. IL DIRITTO/OBBLIGO DEL MEDICO A NAVIGARE IN SICUREZZA

Il professionista sanitario custodisce sui suoi *device* tantissimi dati personali e sanitari dei propri pazienti, preda ghiotta e ambita per hacker e criminali informatici; così come non lascerebbe lo studio con la porta aperta e le prescrizioni alla mercé di chiunque, allo stesso modo deve cercare – per quanto possibile – di chiudere a chiave, o quantomeno filtrare il più possibile, le proprie tracce online. Per un hacker o un esperto informatico rubare i dati online è più facile di quanto sembri, molto più che rubare caramelle a un bambino.

3.1 CHIUDERE A CHIAVE TUTTO CON PASSWORD FORTI

Per usufruire di qualunque servizio sul web bisogna essere dotati di una username (di solito la nostra e-mail) e di una *password*, che dovrà essere forte, in modo da non correre il rischio che venga forzata da malintenzionati che potrebbero entrare nella nostra e-mail, nel nostro profilo social, nel nostro software online di gestione dei dati dei pazienti, sottraendo i nostri dati o compiendo operazioni fraudolente a nostro nome.

Mai utilizzare come *password* il semplice 0000 oppure 1111, o le combinazioni nome cognome e data di nascita: queste ultime informazioni, per un medico – e in generale per un professionista iscritto a un albo – sono di dominio pubblico, facilmente consultabili dall'Albo online, il primo posto in cui un hacker va a cercare i nostri dati per cercare di entrare nelle nostre vite online, confidando in una password fatta dalla nostra data di nascita. Se fossi un hacker e volessi attaccare i vari profili del dottor Mario Rossi, per prima cosa andrei, infatti, a cercare informazioni online, riuscendo a carpire dati personali dall'albo e informazioni professionali e personali dai suoi profili social e dal suo sito. Se malauguratamente il dottor Mario Rossi ha inserito come password per tutti i suoi profili la sua data di nascita 01/01/1901 o la sua data di iscrizione all'albo dei medici, il gioco sarebbe estremamente semplice per il criminale informatico.

La raccomandazione è quello di creare **password complesse**, formate da combinazioni di almeno 15 caratteri di lettere, numeri, caratteri speciali maiuscole e minuscole. Come dice un famoso articolo di Troy Hunt del 2011, ***The only secure password is the one you can't remember***: la password più sicura è perciò quella impossibile da ricordare.

Le password devono, naturalmente, essere custodite gelosamente. Inutile creare una password forte per accedere, ad esempio, alla casella di posta elettronica se poi, durante una call per un'intervista, una videoconferenza o un video divulgativo online la password è in bella mostra sul post it attaccato al computer, in mondovisione. Le modalità di conservazione delle password sono molteplici: i meno tecnologici possono decidere di creare la classica rubrica delle password cartacea, da tenere gelosamente sottochiave. I più tecnologici, invece, possono ricorrere ai *password manager*, cioè programmi o app che archiviano in modo sicuro – e soprattutto crittografato – le credenziali di accesso ai servizi web in una specie di cassaforte virtuale, resa disponibile all'utente quando ne ha bisogno

3.2 INSTALLARE UN BUON ANTIVIRUS

L'antivirus rappresenta il principale strumento di protezione dagli attacchi che una macchina (computer, smartphone) potrebbe subire navigando sul web. La raccomandazione è quella di scaricare solo ed esclusivamente programmi antivirus originali da siti sicuri (che utilizzino il protocollo https) o comunque dall'Apple store o da Play store nel caso di smartphone.

Per poter funzionare correttamente, la versione antivirus installata dovrà essere sempre quella più recente e le definizioni dei virus/malware dovranno essere costantemente aggiornate.

3.3 IL BROWSER WEB

Il *browser* web che utilizziamo per navigare, sia sul cellulare che dal computer, deve essere sempre aggiornato all'ultima versione disponibile: gli aggiornamenti, infatti, permettono di eliminare eventuali bug di sicurezza. Solitamente i browser web si aggiornano in automatico, ma è bene, ogni tanto, verificare che le loro impostazioni di aggiornamento.

Nell'utilizzare un *browser* è molto importante, inoltre, proteggere la propria privacy. Non tutti sanno, ad esempio, che attraverso la cosiddetta tecnica del fingerprinting i browser prendono una vera e propria impronta digitale della macchina da cui avviene il collegamento a internet e del *browser*, identificando completamente o parzialmente sia l'utente che il dispositivo, riconoscendo l'indirizzo IP e molti altri dati. Si tratta di un metodo di tracciamento online estremamente diffuso, molto più invasivo dei classici *cookie* che troviamo all'ingresso di un sito web. Attraverso la *fingerprinting* una persona può essere tracciata per mesi, anche dopo aver eliminato ogni dato dal *browser.* In alcuni casi la *fingerprinting* può avere un utilizzo "buono", come quando c'è un tentativo di accesso alla nostra e-mail o all'internet banking da un dispositivo nuovo, sconosciuto e potenzialmente criminale.

Un utile suggerimento è quello di **proteggere la propria privacy online** utilizzando dei **browser web** sicuri che proteggano da tracciamento, *fingerprinting*, *phishing*, *hacking* della *webcam* e dispongano di una modalità sicura per effettuare l'accesso all'*internet banking* (la cosiddetta Modalità Banca), come ad esempio i *browser* proposti dai produttori di antivirus oppure optando direttamente per il Tor browser o Duck Duck Go sullo smartphone. Va specificato, però, che questo tipo di browser offre risultati di ricerca meno accurati e una navigazione più lenta rispetto al classico Google Chrome (il più utilizzato al mondo, nonostante non brilli per il rispetto della privacy degli utenti).

3.4 NON APRIRE QUELL'E-MAIL

Uno dei pericoli principali, nell'utilizzo del web, è quello di ricevere e-mail di phishing: si tratta di una tipologia di truffa online attraverso la quale l'attaccante cerca di ingannare la sua vittima convincendola a fornire informazioni personali, dati finanziari, codici d'accesso, fingendosi un contatto o un ente conosciuto dalla vittima.

Le e-mail di phishing più riconoscibili sono quelle con le finte richieste d'aiuto da parte di contatti a noi noti: dall'e-mail di un nostro familiare ci arriva un messaggio, solitamente sgrammaticato, in cui si dice che il nostro caro è in pericolo e ha bisogno di un bonifico immediato o di un versamento in bitcoin per poter risolvere il suo problema. La maggior parte delle e-mail è dotata di un filtro anti-phishing e anti-spam, ma nel caso in cui questi non funzionassero a dovere, si raccomanda di cestinare immediatamente questa tipologia di e-mail senza nemmeno aprirle.

Il *phishing* non riguarda solo le e-mail, ma anche gli sms e le chat di messaggistica istantanea, come WhatsApp. È proprio degli ultimi mesi la cosiddetta truffa del figlio in difficoltà: la vittima riceve via Whatsapp un messaggio con scritto *"Ciao papà. Mi è caduto il telefono, questo è il mio nuovo numero, per cortesia mi mandi un whatsApp?"*. Solitamente il messaggio include un link con un collegamento ipertestuale, e nel caso in cui la vittima clicchi su quel link la truffa è avviata. Inizia lo scambio di messaggi tra il padre e il finto figlio, con richieste di soldi per far fronte a necessità impellenti, giustificate dall'impossibilità di accedere alla propria app bancaria, fuori uso dopo la caduta del cellulare e il cambio del numero.

Riconoscere i tentativi di truffa online diventa sempre più difficile, perché i criminali imparano dagli errori commessi. Il suggerimento è quello di stare sempre all'erta e verificare, quando si ha un dubbio sull'e-mail o sul messaggio ricevuto, la presenza di alcuni piccoli campanelli d'allarme:

- **controllare il numero di telefono del mittente** • se, ad esempio, si riceve un messaggio da un ente (come la Banca) da un numero che è diverso da quello utilizzato abitualmente per le comunicazioni, sicuramente sarà un tentativo di truffa;
- **attenzione al mittente che mette ansia e fretta** • se il contenuto dell'e-mail o del messaggio tende a generare ansia e fretta nell'erogazione di somme di denaro, stare molto attenti prima di rispondere o di cliccare su eventuali link presenti nel messaggio, perché potrebbe essere un tentativo di truffa;

controllare i link • quando un'e-mail o un messaggio contiene un link ipertestuale e non siamo sicuri del mittente, nel dubbio è sempre meglio evitare di cliccarci sopra; per verificarne l'autenticità un suggerimento è quello di passare il puntatore del mouse sul link, se si tratta di un sito vero, dovremmo vedere l'anteprima e l'indirizzo web a cui conduce.

attenzione agli errori di ortografia • di solito i messaggi contenenti tentativi di truffa contengono degli errori di ortografia o un uso stravagante della punteggiatura (per esempio virgole al posto dei punti, mancanza di maiuscole); in questi casi, è bene cestinare il messaggio ed evitare di rispondere o cliccare sul link che ci è stato inviato.

Navigare in sicurezza sul web è difficile ma non impossibile: con un po' di formazione e un po' di attenzione il professionista medico può dormire sonni tranquilli.