05/2020

CIRCULAR AMB RECOMANACIONS AL VOLTANT DE LA TELEASSISTÈNCIA

Al nostre entorn sanitari i social, la situació actual d'excepcionalitat ha fet necessari desenvolupar nous models d'actuació i assistència per minimitzar l'exposició al contagi tant del personal sanitari com dels propis pacients i usuaris.

Hem de considerar també que davant la desescalada progressiva els centres poden necessitar combinacions entre diferents models d'atenció (*presencial i teleassistència en qualsevol de les seves modalitats, per atenció telefònica o per vídeo conferència*) per poder mantenir mínims nivells d'activitat.

L'atenció virtual o telefònica o mitjançant vídeo conferència es revelen com a mitjans adequats per aconseguir minimitzar riscos d'exposició durant el procés de retorn a la normalitat, que es preveu sigui llarg, no descartant-se hores d'ara que sigui una metodologia i via d'atenció que s'estableixi ja de forma definitiva convivint amb les visites presencials.

No parlem d'un tractament de dades diferencial al propi i central del que realitzen les entitats sanitàries (activitat assistencial) sinó (i no sempre) d'un nou canal a través del qual es realitza aquest tractament.
En aquest sentit recomanem als centres:

a. Recomanem un esforç especial en la política d'informació sobre la implantació dels nous canals d'assistència al pacient, garantint el principi de transparència propi de les polítiques de protecció de dades, que hauria d'incloure el recordatori de la prohibició d'enregistrar de qualsevol manera les visites que es portin a terme per aquesta via.

b. Sovint la teleassistència se serveix de plataformes tecnològiques que requereixen una avaluació d'impacte, en els termes previstos en l'article 35 RGPD. Per tant, el responsable del tractament haurà de garantir en la major brevetat possible disposar del degut informe i implementar les mesures de seguretat que en derivin.

c. Revisar els procediments / protocols per garantir la seguretat, concretament pel que fa a la confidencialitat de les dades del pacient, i assegurar que el personal hagi signat el compromís de confidencialitat i el manual de bones pràctiques, o document equivalent. Preveure que el personal notifiqui les incidències de seguretat (per detectar eventuals fuites de seguretat)

d. Avaluar la seguretat de les connexions, aspecte que recomanem treballar amb les Àrees de Sistemes. També convé treballar aspectes com disposar d'usuaris individuals, control d'accés amb contrasenyes robustes (amb criteris de canvi periòdic i previsió de bloqueig per error davant vulnerabilitats d'àtacs de força bruta), disposar d'un bloqueig per inactivitat de minuts, disposar d'antivirus i/o Firewall, sistemes de detecció d'intrusos, controls d'accessos eines per a l'emmagatzemat i impressions de la informació i dades personals. En cas que el programa sigui prestat per un proveïdor extern, caldrà analitzar les mesures de seguretat del proveïdor, la localització de les dades, si es realitzen transferències internacionals de dades, etc.

e. Recordar que aquests processos d'atenció formen part de la prestació assistencial, i per tant és convenient tenir cura de traslladar a la HC la informació i les indicacions efectuades pels professionals durant les sessions amb els pacients.

Al marge d'aquestes consideracions, resulta recomanable que les organitzacions sanitàries i socials estableixin polítiques corporatives per la implantació d'aquestes vies d'assistència, que vetllin per un seguiment i implementació adequada a les condicions de seguretat de les dades, que evitin per altra banda el perjudici per als usuaris afectats per la bretxa digital i que en darrer terme no generin situacions de manca d'equitat en el tractament.

Serveis de Protecció de Dades
Codi Tipus
Fundació Unió Catalana d'Hospitals
coditipus@uch.cat

Barcelona, 30 d'abril de 2020