Recomendaciones para profesionales para el uso correcto de las TICs de la Sociedad Española de Cuidados Paliativos Pediátricos (PEDPAL)

1. INTRODUCCIÓN. DEFINICIONES

Las TIC han inundado absolutamente todas las esferas de la vida del ser humano.

El **concepto TIC** engloba pues todos aquellos servicios basados en:

- el intercambio de información (correo electrónico, productos audiovisuales, foros y redes sociales, buscadores de información …)
- las redes de telecomunicaciones que dan soporte a dicho intercambio de datos (telefonía fija y móvil, internet, intranets corporativas …)
- los terminales empleados para poder acceder a los distintos servicios (ordenadores personales, teléfonos, smartphones, tablets, reproductores de audio y vídeo…)

Dentro del amplio espectro que abarca el concepto TIC aparece en los últimos años la llamada **«salud electrónica» o e-Salud (eHealth)**, definida como el conjunto de técnicas y dispositivos empleados para el tratamiento y la transmisión de información sobre salud, y dentro de ella se expanden nuevos campos, como la historia clínica electrónica (HCE) o la telemedicina.

El **concepto de mHealth o Salud móvil** (englobado a su vez en eHealth o e-Salud) hace referencia a las aplicaciones móviles enfocadas en la salud, dirigidas tanto a profesionales cómo a pacientes y suponen herramientas de ayuda al seguimiento.

La sanidad móvil permite la monitorización del paciente en su entorno y facilita la recogida de un considerable número de datos médicos personales, así como el acceso de los pacientes a su propia información sanitaria. Aunque el gran número de aplicaciones que han irrumpido de forma tan rápida, hace que buena parte de las aplicaciones que se descargan no hayan sido acreditadas con garantías de calidad y seguridad.

Por todo ello, es necesario establecer controles de calidad que permitan que médicos y pacientes puedan utilizar esta tecnología con completa seguridad para la reducción de posibles errores médicos y la protección de los pacientes.

2. CLASIFICACIÓN DE LOS SERVICIOS DE TELEMEDICINA

Tipo de servicio de Telemedicina se va a ofrecer. En función de la clasificación hecha por The National Center for Biotechnology Information (NCBI) los servicios se pueden clasificar de tres formas:

1. **Síncrono**: servicio que se ejecuta en tiempo real. Ello permite un contacto in vivo entre el profesional sanitario y paciente.

2. **Asíncrono:** solución online o basada en una solución de chat que permite conectar con los pacientes para compartir información sobre su salud para que el profesional la pueda revisar más tarde, o permite compartir a un profesional sanitario la historia clínica digital, imágenes y otros informes clínicos de un paciente con otro profesional sanitario especialista para obtener una opinión en base a su conocimiento y experiencia, y así obtener un mejor diagnóstico o un tratamiento.

Permite personalizar preguntas en función de los protocolos clínicos para recopilar información importante sobre los síntomas o el estado de salud de un paciente.

3. **Telemonitorización**: evaluación en tiempo real del estado clínico de un paciente, bien a través de una monitorización directa por vídeo o a través de datos personales de salud y las imágenes que se tengan del mismo. El uso de apps permite tener muchos parámetros sobre el estado del paciente en cualquier momento y es una opción claramente emergente.

3. RECOMENDACIONES TÉCNICAS

Para poder realizar Telemedicina es fundamental contar con las infraestructuras necesarias, teniendo en cuenta que el sistema sea eficiente y dé respuesta a las necesidades del profesional y del paciente. Las recomendaciones técnicas para poder establecer una conexión de calidad van a depender de las comunicaciones y de los equipos.

- Recomendaciones de las comunicaciones para el profesional sanitario:
    - infraestructura estable que facilite altos anchos de banda, baja latencia y estabilidad del servicio a lo largo del tiempo
    - preferentemente, comunicación por cable entre el router y el equipo en el que se va a realizar la videoconferencia, evitando las conexiones WiFi

- contratación de servicios con acuerdos de nivel de servicio (SLA) garantizados, huyendo de los servicios estándar dirigidos a gran consumo
- disponibilidad cuando sea posible de un router 4G independiente, como garantía ante indisponibilidades del servicio

- Hasta que las comunicaciones 5G se desarrollen suficientemente, la opción preferencial para el para el paciente serán las comunicaciones por fibra óptica en el hogar (FTTH).
- Para los equipos, dependerán fundamentalmente de la solución de videoconferencia elegida, debiendo seguir sus especificaciones, prestando especial atención a los apartados de memoria, CPU, necesidad de GPU independiente, disco de estado sólido, etcétera.

4. SEGURIDAD DE LOS DATOS

Las cuestiones relativas a seguridad se establecen en dos aspectos fundamentalmente:

- Protección y seguridad de los datos.
- Funcionamiento seguro que no afecte negativamente a la salud del paciente

Cada país aplica sus propias normativas para regular la *e-salud*, pero en todos ellos, la privacidad de la información médica es un derecho que debe ser respetado.

La ciberseguridad es la llave de la era digital, sin ella resultaría imposible avanzar en materia de digitalización. Cuando la digitalización afecta al ámbito sanitario las necesidades de ciberseguridad aumentan, y sus implicaciones son muy amplias: desde proteger la propiedad intelectual de un medicamento o almacenar los resultados de un ensayo clínico hasta garantizar la privacidad de un paciente individual.

Los datos médicos de carácter personal son la información más sensible que existe, y tanto los profesionales médicos como los centros hospitalarios y los sistemas de salud están obligados por ley a garantizar su confidencialidad.

Reglas para preservar la seguridad de los datos médicos y a evitar fugas de información:

- **Cifrado de la información**

El almacenamiento seguro de la información es una tarea crítica, y por eso debe adoptar todas las medidas a su alcance para garantizarlo. Una de las más eficaces consiste en el cifrado de los datos, y en la actualidad casi todos los sistemas operativos incluyen alguna de forma nativa.

- **Contraseñas robustas**

El uso de contraseñas seguras es una constante en las recomendaciones que hacen los responsables de seguridad informática. Solo hay que recordar que estas claves suelen ser el principal obstáculo que tienen los piratas para poder acceder a información sensible almacenada en los equipos informáticos, en los terminales móviles y en la nube. Por eso es recomendable seguir algunas pautas:

· La contraseña debe tener 12 caracteres alfanuméricos.

· Se deben usar contraseñas diferentes en el ámbito personal y en el profesional.

· La clave no debe incluir fechas de cumpleaños, el nombre de los hijos, etc.

· No se debe compartir por ningún medio digital.

- **Instalación de antivirus**

Los antivirus son muy importantes para evitar infecciones por *malware*, es decir, software malicioso con el que los piratas acceden a los equipos sin que su propietario se dé cuenta. Un buen antivirus es capaz de detectar y frenar todas estas amenazas para reducir el riesgo de fuga de información.

- **Hacer una copia de seguridad**

Es indispensable hacer una copia de seguridad de todos los datos sensibles, que también deben estar cifrados. Además, es conveniente guardarla fuera del alcance de personas no autorizadas y físicamente lejos de donde se encuentra la información original.

- **Borrado seguro**

Toda la información que se almacena en un equipo informático deja un rastro que solo se puede eliminar de manera definitiva a través de un borrado seguro. Para hacerlo es necesario utilizar herramientas de terceros que se pueden encontrar de forma sencilla en internet o recurrir a un profesional o empresa especializada.

- **Utilizar una conexión segura**

Las redes WiFi públicas carecen de la seguridad necesaria para acceder con garantías a la intranet de la empresa o a un correo profesional o corporativo. Para hacerlo con seguridad desde fuera del ámbito laboral se puede usar una red privada virtual o VPN, una conexión que permite acceder a internet con seguridad.

5. REQUISITOS DEL LUGAR DONDE REALIZAR LA TELEMEDICINA

Es fundamental garantizar que el paciente, su familia, y el profesional tengan un espacio cómodo para poder establecer una buena conexión. Para esto, es muy importante comprobar previamente a la puesta en marcha de cada visita que las conexiones son adecuadas y que el paciente conoce mínimamente cómo conectarse y cómo manejar la tecnología, de ahí la importancia de una formación previa a la puesta en marcha de un programa de Telemedicina.

Algunas de las consideraciones principales son las siguientes:

- Espacios libres de interrupciones. Asegurar en todo momento la privacidad. No presencia de terceras personas.
- Lugar tranquilo, con fondo lo más neutro o relajante posible. No tener nunca comida, ni bebidas visibles a la cámara.
- Se debe de establecer una atmósfera lo más profesional posible, así, se debe de ir con indumentarias profesionales como si se estuviera en la visita presencial.
- Que la cámara esté situada para permitir un mismo nivel entre los ojos del paciente, su familia y los del profesional.

6. ASPECTOS ÉTICOS Y LEGALES PARA EL USO DE LA TELEMEDICINA

Consideraciones basadas en las reglas (artículo 26) del Código de Deontología Médica de 2011:

- El ejercicio clínico de la medicina mediante consultas exclusivamente por carta, teléfono, radio, prensa o Internet es contrario a las normas deontológicas. La actuación correcta implica ineludiblemente el contacto personal y directo entre el médico y el paciente.
- Es éticamente aceptable, en caso de una segunda opinión y de revisiones médicas, el uso del correo electrónico u otros medios de comunicación no presencial y de la telemedicina, siempre que sea clara la identificación mutua y se asegure la intimidad. Los sistemas de orientación de pacientes, mediante consulta telefónica o telemedicina, son acordes a la deontología médica cuando se usan exclusivamente como una ayuda en la toma de decisiones.
- Las reglas de confidencialidad, seguridad y secreto se aplicarán a la telemedicina en los mismos términos establecidos en el Código de Deontología para el ejercicio de la medicina convencional.

Todos los requisitos señalados constituyen normas de obligado cumplimiento que las organizaciones tendrán que garantizar para la implantación de programas de telemedicina, quedando la responsabilidad de los profesionales limitada al mero ejercicio profesional.

El uso de la telemedicina, cualquiera que sea el ámbito en el que se desarrolle, tiene que estar sujeto a unas normas (Sánchez Caro y Abellán 2002). Resumidamente los **requisitos que deben darse para la telemedicina** son:

a) El uso de la telemedicina se legitima por el beneficio al paciente, pero nunca por la mayor comodidad exclusiva del médico.

b) Es preciso obtener el consentimiento del paciente, y con el fin de evitar los riesgos de fuga de información inherentes a las comunicaciones electrónicas deberá asegurarse la adopción de las normas de seguridad que garanticen la confidencialidad del paciente, en un doble sentido:

• Los datos relativos al paciente y otras informaciones que le conciernen no pueden ser transmitidos a un médico o a otro profesional de la salud más que a petición del paciente, o con su consentimiento, y en la medida en que él determine.

• Las informaciones que se transmitan deben referirse al problema médico concreto de que se trate.

c) Es relevante la conservación en la historia clínica, quedando debidamente documentados, tratando de garantizar la perennidad, así como su seguridad y la recuperación de la información.

d) Los profesionales intervinientes deben encontrarse autorizados para ejercer y ser competente en su especialidad médica.

7. FORMACIÓN PREVIA A LA PUESTA EN MARCHA DE LA TELEMEDICINA

Para que tenga éxito y funcione un programa de Telemedicina, es imprescindible dedicar un tiempo a la formación de los profesionales sanitarios que van a desarrollar el servicio, y también a los pacientes y familias que vayan a participar. Los profesionales deben conocer y aprender a manejar la tecnología, y como realizar la atención al paciente y su familia en ese tipo de visita no presencial.

Es conveniente elaborar unas **guías de formación y de uso** del programa a implantar, para facilitar el uso de la tecnología a los profesionales y a las familias. Las guías una vez elaboradas, deben difundirse entre los profesionales que van a intervenir en el programa de Telemedicina y posteriormente con cada uno de los pacientes y familias que van a ser atendidos mediante este sistema.

También puede resultar útil y práctico la creación de un **vídeo explicativo**, dirigido tanto a los profesionales, como especialmente a las familias, que recopile los puntos básicos de la guía que se elabore. Otra opción alternativa sería la elaboración de una presentación tipo 'PowerPoint', o cartelería como apoyo a la guía para el profesional y las familias.

8. DOCUMENTAR LA INFORMACIÓN CLÍNICA

Los datos y la información obtenidas a través de las visitas no presenciales deben documentarse e integrarse en la historia clínica digital, es decir, deben de ser tratados como en el caso de la presencial. Se recomienda reflejar la visita realizada en el curso clínico del paciente, como lo haríamos en una visita presencial. Para esto, es necesario que exista ya una historia clínica digital en el centro donde está vinculado el profesional que realiza la visita no presencial, y sea en esta historia clínica digital donde se anote la visita.

Existen plataformas de Telemedicina que resultan fáciles de integrar en los Sistemas de información de centros o de sistemas de salud.

9. EVALUACIÓN Y SEGUIMIENTO DE LA TELEMEDICINA

Para poder evaluar la atención que se realiza a través de un programa de Telemedicina, es imprescindible tener un seguimiento de esta actividad, de la misma forma que se tiene con cualquier actividad asistencial desarrollada por profesionales sanitarios.

Por ello deben crearse algunos indicadores (KPI, Key Performance Indicator) para poder hacer el seguimiento correctamente. Indicadores que podemos utilizar:

- Clínicos: patología de base, nivel de cuidados y soportes que precisa
- Consumo de recursos sanitarios: ingresos hospitalarios, GRD, consultas a las UCPP, visitas a urgencias, nº de consultas al especialista, visitas a domicilio, consultas por videoconferencia, tiempo de la consulta por videoconferencia, etc.
- Satisfacción de los pacientes y sus familias: mediante alguna encuesta estructurada o utilizando algún tipo indicador de satisfacción como el sistema NPS (Net Promote Score).

Ejemplos:

- Número de visitas no presenciales en un tiempo determinado (día/mes/año).
- % de visitas no presenciales/total de visitas, para evaluar la transformación digital
- Número de cancelaciones. % de cancelaciones sobre las visitas no presenciales. Es importante comparar este indicador con el de visitas presenciales, para saber la eficacia en cuanto a asistencia en un modelo o en otro.

10. BIBLIOGRAFÍA

- Asociación de Salud Digital. Guía básica de recomendaciones para la Teleconsulta. Mayo 2020. Disponible en: http://salud-digital.es/wp-content/uploads/2020/05/Guia_ASD_mayo2020.pdf
- Bataller A, Cassasa A, de Carreras LL, Martínez M, Moro M, Pidevall I, et al. Recomendaciones sobre el uso de información médica y el ejercicio de la libertad de expresión en las redes sociales. Consejo de Colegios de Médicos de Cataluña. Disponible en: http://www.medicosypacientes.com/sites/default/files/RECOMENDACIONES%20SOBRE%20EL%20USO%20DE%20INFORMACI%C3%93N%20M%C3%89DICA%20Y%20EL%20EJERCICIO.PDF
- Asociación Médica Mundial. Aspectos éticos en el uso de la Telemedicina. 69ª Asamblea General de la WMA. Julio 2020. Disponible en: https://www.wma.net/es/policies-post/declaracion-de-la-amm-sobre-la-etica-de-la-telemedicina/
- ATA'S QUICK-START GUIDE TO TELEHEALTH DURING A HEALTH CRISIS https://www.jshfirm.com/wp-content/uploads/2020/04/ATA_QuickStart_Guide_to_Telehealth_4-10-20.pdf
- Sánchez Caro J, Abellán F. Telemedicina y protección de datos sanitarios. Granada: Fundación Salud; 2000. p. 2002.
- Muñoz Fernández L, Díaz García E, Gallego Riestra S. Las responsabilidades derivadas del uso de las tecnologías de la información y comunicación en el ejercicio de las profesiones sanitarias. An Pediatr (Barc). 2020;92(5): 307.e1---307.e6
- Colegio de Psicólogos de Madrid. Guía de intervención psicológica no presencial, 2020. Disponible en: https://www.psi-onlife.es/wp-content/uploads/2020/03/Protocolo-breve-Intervencio%CC%81n-Psicolo%CC%81gica-no-presencial_.pdf
- Organización Médica Colegial. Ética y Redes Sociales. Manual de estilo para médicos y estudiantes de medicina. Sobre el buen uso de las redes sociales. OMC. Consejo General de Colegios de Médicos de España. Disponible en: https://www.cgcom.es/sites/default/files/u183/Manual%20Redes%20Sociales%20OMC.pdf