

NUEVAS MODALIDADES DE SERVICIOS MÉDICOS
E-HEALTH Y M-HEALTH: FRONTERAS LEGALES Y ESPACIOS DE
EJERCICIO

Isabel Koutsourais Fernández
Máster Derecho Sanitario y Bioética

Fecha de publicación: 22 de abril de 2015

Contenido

1.	INTRODUCCIÓN	3
2.	PROBLEMAS DE BASE A SER RESUELTOS.....	6
3.	GASTO SANITARIO:	7
4.	NORMATIVA APLICABLE:	8
5.	MEDIDAS PARA IMPULSAR EL DESARROLLO DE LAS TIC EN EL ÁMBITO SANITARIO.....	10
5.1	A NIVEL EUROPEO:.....	10
a)	e-Health Action Plan 2012-2020.....	10
5.2	A NIVEL NACIONAL:.....	11
a)	Informe del Consejo Asesor de Sanidad	11
b)	Plan de Telemedicina 2014-2018:.....	13
c)	Sociedad Ibérica de Telemedicina y Teleconsulta (SITT):	13

6.	INFORMACIÓN Y PROTECCIÓN DE DATOS:	13
7.	HISTORIA CLÍNICA:.....	16
8.	SEGURIDAD DEL PACIENTE:	17
9.	CORRECTA IDENTIFICACIÓN DE LAS PARTES INTERVINIENTES:.....	18
10.	RESPONSABILIDAD DE LOS PROFESIONALES INTERVINIENTES:	19
11.	APLICACIONES SANITARIAS (M-HEALTH):	20
12.	ASISTENCIA SANITARIA TRANSFRONTERIZA.....	25
13.	OTROS USOS DE LAS TIC: VENTA A DISTANCIA DE MEDICAMENTOS	26
14.	CONCLUSIÓN	27
15.	BIBLIOGRAFÍA:	28

1. INTRODUCCIÓN

El presente trabajo busca llevar a cabo un pormenorizado análisis de los diferentes interrogantes jurídicos que se plantean en el auge y aplicación de las nuevas tecnologías en salud, así como cuales son las respuestas y próximos pasos a dar en este ámbito. Esta **nueva forma de ejercer la medicina**, está provocando toda una revolución en la práctica clínica asistencial, que hace necesario **dotar de uniformidad** a los diferentes instrumentos normativos.

Desde un principio el concepto de telemedicina ha sido definido como medicina ejercida en la distancia. Pero la Asociación Norteamericana de **Telemedicina** (ATA) habla de un *“intercambio de información médica desde un punto hacia otro por medio de las comunicaciones electrónicas con el objeto de mejorar el estado de salud de un individuo”*.

Con esto hay que ligar el concepto de **e-Health**, que incorpora los conceptos de servicios y atención sanitaria, gestión y educación, así como el de informática médica que sirve como base para implementar las aplicaciones en salud y el de **m-Health**, que hace referencia a las prácticas de salud realizadas a través de dispositivos móviles.

Pero se hace necesario ir más allá del concepto tradicional, interpretando que la aplicación de las nuevas tecnologías en la sanidad se posiciona como un nuevo instrumento para salvaguardar la salud de las personas.

Así la OMS define la telemedicina como: *“el suministro de servicios de atención sanitaria en los que la distancia constituye un factor crítico, por profesionales que apelan las TICs con objeto de intercambiar datos para hacer diagnósticos, preconizar tratamientos y prevenir enfermedades y heridas, así como para la formación permanente de los profesionales de la atención de la salud y en actividades de investigación y evaluación, con el fin de mejorar la salud de las personas y de las comunidades en que viven”*

Lo trascendente es el cambio del modelo de atención sanitaria que está produciendo el acceso a las nuevas tecnologías, que permiten eliminar las barreras de tiempo y distancia, pasando a crear un sistema accesible en tiempo y forma a todo aquel que lo necesite o participe del mismo. Esta integración ha generado un cambio en la manera en la que se proporciona y recibe información y servicios para el cuidado de la salud, lo

que lleva a que se planteen nuevas formas de comunicación y tipos de práctica que plantean **problemas éticos y legales**.

La telemedicina implica la transmisión segura de datos e información médica a través de texto, sonido, imágenes u otras formas necesarias para la **prevención**, el **diagnóstico**, el **tratamiento** y la **vigilancia** del paciente y en este sentido cobran especial importancia las reglas éticas y profesionales relativas a la prestación de este tipo de servicios. Por todo ello, el término telemedicina está cediendo el paso a uno más amplio: la eHealth o Telesalud.

La evolución de las tecnologías hace que la e-Health y la m-Health evolucionen a sistemas cada vez más complejos en su estructura interna y en su relación con los sistemas del propio ámbito sanitario (Historia Clínica Electrónica, receta electrónica, cita previa, etc), y otros sistemas externos tales como la educación, la industria, el sector de las telecomunicaciones o los servicios sociales, siempre teniendo presente que el tema central es la seguridad del paciente.

El establecimiento de **estrategias** en e-Salud, ha ido creciendo en protagonismo desde que el pasado año 2005, la Organización Mundial de la Salud recomendara a los Estados a incorporarlas a sus políticas sanitarias dado su impacto positivo en el fortalecimiento de los sistemas de salud y la mejora en la calidad, seguridad y acceso a la asistencia sanitaria.

Las funcionalidades que el desarrollo de las TIC en Salud ofrece son muchas:

- **Comunicación directa** con el paciente mediante videoconferencia en tiempo real
- **Control de parámetros** fisiológicos y biométricos (tensión, nivel de saturación de oxígeno, ritmo cardiaco)
- Asistencia y **seguimiento continuo** de pacientes crónicos o personas dependientes
- **Rehabilitación** remota y seguimiento de la misma
- **Registro y almacenamiento de datos**, bien de forma automática (mediante dispositivos) bien manual, introduciendo el paciente los datos en una web.

Partiendo de las funcionalidades aquí expuestas, se establecen diversas modalidades de telemedicina tales como la telemonitorización, el telediagnóstico, la telerehabilitación o teleformación entre otras.

El motivo principal que me ha llevado a la elección del tema, ha sido además de la actualidad del mismo (dado el proceso de cambio continuo y tecnológico en el que nos encontramos inmersos), la heterogeneidad de respuestas éticas y legales que he encontrado a cuestiones relativas a la aplicación de las nuevas tecnologías en salud. Cuestiones que precisan establecer un **marco de actuación homogéneo** para dotar de seguridad tanto al profesional como al paciente, puesto que no es suficiente extrapolar las normas existentes en el entorno offline al mundo online porque da lugar a situaciones de difícil interpretación jurídica y vacío legal.

En España, se han logrado avances en el ámbito de la eHealth, sobre todo en la adopción de la Historia Clínica Digital del Sistema Nacional de Salud y en la implantación de la receta electrónica. En la actualidad existen casi 20 millones de historias clínicas y más de un 70% de recetas electrónicas, pese a ello las desigualdades en las diversas CCAA son patentes.

La interoperabilidad, accesibilidad, la identificación segura de los participantes, la protección de los datos, la estandarización terminológica, la cultura digital y el trabajo en red son alguna de las cuestiones que tal y como establece el Informe del Consejo Asesor de abril de 2014, debe dar respuesta la **Estrategia de e-Salud** que se desarrolle en España.

En el presente trabajo se abordarán los siguientes capítulos:

1. Problemas de base a ser resueltos
2. Gasto sanitario
3. Normativa aplicable
4. Medidas para impulsar el desarrollo de las TIC en el ámbito sanitario: a nivel europeo y a nivel nacional
5. Información y protección de datos
6. Historia Clínica
7. Seguridad del paciente
8. Correcta identificación de las partes intervinientes
9. Responsabilidad de los profesionales intervinientes
10. Aplicaciones sanitarias
11. Asistencia Sanitaria Transfronteriza
12. Otros usos de las nuevas tecnologías: Venta a distancia de medicamentos
13. Conclusiones

Cabe resaltar, que este trabajo de investigación no sólo está centrado en las funcionalidades de la eHealth, sino en definir los **límites legales y espacios de ejercicio** de todas las nuevas formas de ejercer la medicina que nos brindan las nuevas

tecnologías, ya que existe un gran vacío legal sobre los derechos y obligaciones derivados de las partes en la atención online, el consentimiento del paciente tratado y la privacidad de los datos personales de carácter sanitario.

Vacío legal que debe ser cubierto ya que la aplicación de las TIC en el ámbito sanitario se impone como un **instrumento clave** para lograr una sanidad más **sostenible** y de **calidad** aún con las limitaciones de recursos existentes en nuestros días y como un medio para **mejorar la salud** de las personas.

2. PROBLEMAS DE BASE A SER RESUELTOS

Se puede observar en la literatura que la mayor parte de las alusiones a este tema están centradas casi en exclusiva en la protección de datos, la confidencialidad y la seguridad del paciente. Pero asimismo hay que tener en cuenta los riesgos aumentados para la seguridad de custodia de los datos y la privacidad por **cuestiones técnicas y de sistemas**, los **errores** humanos, y las **acciones malintencionadas** que aumentan en esta nueva modalidad por el hecho de actuar en entornos fuera del ámbito controlado por las instituciones sanitarias. Y yendo más allá, hay que mencionar todas aquellas **amenazas externas** (catástrofes o accidentes industriales) que pueden poner en juego y afectar a la preservación de salud y la calidad de vida de aquellos pacientes que pudieran depender de un sistema de e-Health.

El sistema sanitario se encuentra en un estado de reformas consecuencia, entre otros factores, del **cambio del entorno organizativo y tecnológico**. Los problemas presentes en la actualidad que deben ser resueltos son:

- La **reticencia al cambio** del sector sanitario
- Las decisiones en materia del mundo de las nuevas tecnologías en sanidad son tomadas sin que exista un **sistema de evaluación** que garantice la efectividad de las mismas.
- Falta de un **enfoque coordinado** en el que puedan extrapolarse los resultados y desarrollar sinergias.
- La aparición de las nuevas tecnologías plantea la necesidad de hacer una reforma en lo que respecta al **modelo de contratación público**, ya que las normas de contratación y pliegos de condiciones no se adecúan a la aparición de situaciones tecnológicas.
- Los proyectos que se plantean en este ámbito necesitan para su desarrollo e implantación de varios ejercicios presupuestarios, no generando **resultados** a

corto plazo por lo que es difícil probar la existencia de beneficios reales en la aplicación de estas tecnologías.

- **Falta de interoperabilidad** técnica, legal y administrativa de los diferentes servicios de telemedicina, haciendo difícil garantizar la calidad y estandarización de los datos en Internet.

Desde un punto de vista técnico, la mayor dificultad radica en la interoperabilidad de los diferentes sectores que intervienen en la eHealth. Los usuarios de estas herramientas, es decir, los profesionales de la asistencia médico-farmacéutica y los pacientes, deberían estar perfectamente capacitados para el uso correcto de cualquier plataforma tecnológica o de sistemas similares en cualquier parte donde pudieran encontrarse (diferentes provincias y CCAA, hospitales de la red nacional, centros de salud, farmacias, etc). La interoperabilidad es crucial tanto en términos de equidad de los diversos tratamientos como en calidad de todos los servicios asistenciales

- Necesidad de medir los niveles de **accesibilidad** a los servicios
- Por último, se debe asegurar una **identificación segura** de todos aquellos que acceden e intervienen en cualquier acto o intervención mediante la red, así es importante saber quién publica datos o facilita una información.

La sanidad electrónica debe fomentar y trabajar para construir la **confianza mutua** entre los actores implicados (pacientes, profesionales sanitarios y proveedores), evitando el riesgo de impersonalidad y falta de atención a los factores psicológicos. La **dimensión humana** debe estar en el centro de la aplicación de las nuevas tecnologías en salud.

3. GASTO SANITARIO:

Desde la Comisión Europea se promueve la sanidad electrónica como medio para **garantizar la continuidad de los tratamientos**, incluso en los desplazamientos de los ciudadanos entre los países de nuestro entorno europeo, y como medio para **mejorar la sostenibilidad** de los sistemas sanitarios.

Según el Comité de Política Económica de la Unión Europea, el coste sanitario relacionado con aquellas personas mayores de 65 años, representa entre el 30 y 40% en los Estados miembros, y su cuota respecto el total de la población aumentaría del 17% en 2010 al 30% en 2060.

En la situación de crisis acaecida en los últimos años, el gasto sanitario ha tendido a crecer por encima del PIB, produciendo una tensión presupuestaria sobre la economía

de las Comunidades Autónomas, donde la Sanidad implica alrededor del 35% del presupuesto de cada Comunidad.

Los factores que incrementan el gasto sanitario son:

- **Incremento de la demanda de servicios:**
 - Progresivo **envejecimiento** de la población, que provoca un mayor consumo de recursos sanitarios (el 80% del consumo de recursos se produce en mayores de 65)
 - Incremento de las enfermedades **crónicas**
- Aumento de los **gastos de infraestructura y recursos humanos**
- **Nuevos avances** en tratamientos y técnicas diagnósticas

En este contexto económico y social de reducción presupuestaria con el aumento de la demanda de servicios en salud donde el modelo sanitario y asistencial se está redefiniendo, se debe perseguir mejorar la **eficiencia** de los recursos, el **conocimiento** de los profesionales y la **accesibilidad y seguridad del paciente**, pero para ello se hace necesario desarrollar innovaciones en los servicios de salud y movernos con todas las **garantías legales** hacia el nuevo paradigma tecnológico que se abre en nuestros días.

Las nuevas tecnologías aplicadas al mundo de la salud, tienen el potencial necesario para hacer frente al aumento del gasto sanitario y al reto demográfico, para contribuir a una mejora general de la salud de los ciudadanos, con más autoasistencia y menor número de hospitalizaciones.

4. NORMATIVA APLICABLE:

Desde hace varios años, los modelos sanitarios de las economías más avanzadas se encuentran en profunda revisión intentando dar respuesta a todos los interrogantes suscitados a raíz del progreso tecnológico, ya que la expansión de las nuevas tecnologías y sus potencialidades en el ámbito de la salud no ha ido acompasado de un **desarrollo normativo** que la dote de seguridad jurídica para que todos los intervinientes (pacientes, profesionales sanitarios y proveedores) gocen de un entorno favorable.

Los aspectos legales y características que se van a analizar en el presente trabajo indican que al hablar de telemedicina nos encontramos por una parte ante un **servicio sanitario**, y por otra ante un **servicio de la sociedad de la información**, por lo que se rige por:

- El principio de libre prestación de servicios

- La normativa de comercio electrónico
- Directiva de derechos de los pacientes en la asistencia transfronteriza

En España no existe una regulación expresa sobre esta materia, pero las normas que son de aplicación son:

- *Ley 16/2003 de Cohesión y Calidad del Sistema Nacional de Salud*
- *Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal así como el Real Decreto 1720/2007 que desarrolla la misma.*
- *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.*
- *Ley 14/1986, General de Sanidad.*
- *Ley 41/2002 de Autonomía del Paciente*
- *Ley 34/1988, General de Publicidad.*
- *Real Decreto Legislativo 1/2007, de la Ley General para la Defensa de los Consumidores y Usuarios*
- *El Real Decreto 81/2014, de 7 de febrero, por el que se establecen normas para garantizar la asistencia sanitaria transfronteriza*

A pesar de la falta de una normativa expresa que regule la práctica profesional de la telemedicina en nuestro país, en Europa se aprobó la Directiva 2011/24/ UE relativa a los derechos de los pacientes en la **asistencia sanitaria transfronteriza**, transpuesta al Ordenamiento Jurídico Español mediante el Real Decreto 81/2014 de 7 de febrero, que sí recoge alguna mención a dicha actividad, y fundamentalmente regula los **derechos de los pacientes** entre los que se incluyen:

- *Recibir tratamiento en otro Estado miembro y ser reembolsado bajo determinadas condiciones.*
- *Tener acceso a una copia de su historial médico por escrito o por medios electrónicos.*

De igual forma, esta Directiva es de aplicación respecto del **registro de los profesionales** de la salud que prestan servicios de telemedicina, y a ella se le unen los artículos 56 y 57 TFUE y la Directiva 2000/31/CE sobre comercio electrónico. En la inmensa mayoría de los países miembros, es la propia organización profesional quien establece las reglas del ejercicio profesional y el control deontológico, por lo que queda

implícito que quien preste servicios de telemedicina cumple con los requisitos de ejercicio profesional del Estado miembro en el que ejerzan su profesión.

En lo que respecta al **procesamiento de los datos relativos a la salud**, la normativa de aplicación es el artículo 16.1 TFUE, el artículo 8 de la Carta de Derechos Fundamentales de la UE, la Directiva 95/46/CE, sobre protección de datos, la Directiva 2002/58/CE, sobre la protección de datos y la privacidad en las comunicaciones electrónicas, y por último la ya mencionada Directiva 2011/24/UE, sobre derechos de los pacientes en la asistencia sanitaria transfronteriza.

Para la **responsabilidad y seguridad derivada de los productos**, la Unión Europea únicamente ha armonizado las reglas relativas a la responsabilidad por productos defectuosos, por lo que en el caso de responsabilidad del profesional sanitario, se aplicará la legislación del Estado miembro de tratamiento. Así, son de aplicación la Directiva 85/374/CE, sobre productos defectuosos, la Directiva 2011/24/UE, asistencia sanitaria transfronteriza, la Directiva 90/385/CE, productos médicos implantables activos y los Reglamentos 593/2008, sobre obligaciones contractuales y 874/2007 obligaciones no contractuales.

La Telemedicina por tanto, es un servicio remunerado, a distancia, llevado a cabo por medios electrónicos a solicitud individual y regida por el principio de país de origen.

La aplicación y extensión de la misma debe estar **alineada con las normas deontológicas** de los profesionales sanitarios, que deberán actualizarse y adaptarse a esta nueva forma de ejercer la medicina. De igual forma, la Ley de Autonomía del Paciente (Ley 41/2002) deberá adaptarse para recoger las nuevas premisas de la telemedicina, tales como el intercambio de información sensible mediante medios telemáticos, el consentimiento informado para este tipo de intervenciones, la custodia, acceso y transmisión de la documentación generada, etc.

5. MEDIDAS PARA IMPULSAR EL DESARROLLO DE LAS TIC EN EL ÁMBITO SANITARIO

5.1 A NIVEL EUROPEO:

a) e-Health Action Plan 2012-2020

La Comisión Europea, desde el año 2004 ha desarrollado diversas iniciativas para impulsar la eHealth a lo largo de los diferentes estados que forman la Unión Europea. Fruto de ello es la hoja de ruta: “*eHealth Action Plan 2012-2020*”, enmarcada dentro

de la Estrategia Europa 2020 que persigue lograr una atención sanitaria inteligente y sostenible para Europa centrada en cuatro puntos clave:

- Puesta en marcha de estrategias para potenciar la **prevención** de enfermedades y la **promoción** de la salud, y **mejora en la gestión** de las enfermedades crónicas
- Desbloqueo de la innovación para dotar de **mayor eficiencia** a los sistemas sanitarios europeos, otorgando más poder al paciente.
- Impulso de la **asistencia sanitaria transfronteriza** y la seguridad sanitaria
- Mejora de las **condiciones legales y de mercado** para todo lo relativo a la eSalud.

5.2 A NIVEL NACIONAL:

Como se ha visto, la eHealth, forma parte de la estrategia de la Unión Europea y de todos los países miembros. En el concreto caso de España, la integración de las **nuevas tecnologías en el ámbito de la salud**, es considerada por el Gobierno Central y por todas las Comunidades Autónomas como una **prioridad**.

Una de las estrategias del Ministerio de Sanidad, Servicios Sociales e Igualdad para ello, es el proyecto de **Sanidad en Línea**, que persigue el impulso de la historia clínica electrónica, la receta electrónica, teleformación, cita por Internet, etc. De forma paralela, las Comunidades Autónomas, han seguido esta línea de priorización, provocando diversidad en lo referente a las cuestiones básicas.

En los próximos años, las políticas del sector sanitario se centrarán en el desarrollo **de sistemas sostenibles**, poniendo foco en la modernización de la infraestructura sanitaria, para que se ajuste a las necesidades sociales.

a) Informe del Consejo Asesor de Sanidad

En abril del pasado 2014, el Consejo Asesor de Sanidad presento su informe: *“La e-Salud, prioridad estratégica para nuestro sistema sanitario”*, que presenta ocho ejes estratégicos de desarrollo:

1. **Mejora de la calidad, eficiencia y continuidad de la Asistencia Sanitaria**, proporcionando recursos que hagan posible una asistencia sanitaria integral para mejorar la seguridad del paciente, la calidad en la atención, la eficiencia y la adherencia al tratamiento en especial de los colectivos sensibles

2. **Interoperabilidad**, de manera que se resuelva la identificación digital de pacientes, profesionales sanitarios y organizaciones, y se amplíe el alcance de la Historia Clínica Electrónica y de la receta electrónica, desarrollando estándares que deben cumplir las soluciones tecnológicas para que puedan ser integradas con los sistemas de información de las organizaciones sanitarias.
3. **Armonización y adecuación de un marco normativo adaptado a la e-salud**
4. **Formación** en conocimientos y habilidades para el uso de las TIC, **comunicación** y **elaboración** de un plan de difusión para involucrar a los diferentes actores. La formación específica de los profesionales sanitarios se establece como uno de los factores clave para el éxito de las iniciativas y para su expansión de forma global y para la seguridad de los actores implicados.
5. **Investigación, desarrollo tecnológico e innovación**, desarrollando sinergias con sectores como el de la farmacia, la biotecnología, la electrónica entre otros y potenciando la colaboración público-privada en el desarrollo de proyectos relevantes del sector.
6. **Dotación de las infraestructuras y de la arquitectura organizativa necesaria** para dar soporte a las nuevas tecnologías, garantizando la seguridad y privacidad de la información y la disponibilidad de servicios con carácter permanente.
7. **Gobernanza**, desarrollando una estructura organizativa transversal en la que se definan las funcionalidades, responsabilidades y competencias para impulsar las acciones y servicios e-salud.
8. **Financiación de la estrategia de e-Salud**, contando con un apoyo financiero coordinado entre los Ministerios, las CCAA y los proveedores de servicios.

Centrándonos en el tercer punto, los objetivos marcados para lograr una armonización y adecuación del **marco normativo** relativo a la e-Salud son:

- Desarrollar, tomando como partida la **confidencialidad** de los datos personales un marco regulatorio que facilite la reutilización de los datos sanitarios para investigación y la iniciativa de datos abiertos.
- Perseguir y potenciar la **armonización** y **adecuación** de la normativa española con la europea.
- **Homogeneizar** las normativas de protección de datos de carácter personal y aquellas disposiciones legales que sean específicas del ámbito de la salud.
- Desarrollar la normativa que persiga promover la continuidad asistencial, eliminando barreras de **intercambio** de información entre centros públicos y privados y permitiendo el intercambio de información de salud.
- Hacer efectivo el **acceso** de los pacientes a su historia clínica y a aquellos servicios que contengan información específica sobre su salud.

- Desarrollar la regulación para el **acceso integrado** a toda la información relevante sobre la salud del paciente, siempre en función de niveles, de responsabilidades y de cometidos profesionales, con independencia de su procedencia, pública o privada e incluyendo el historial farmacoterapéutico, imagen médica y resultados de pruebas complementarias o diagnósticas.
- **Aplicar y adaptar** al ámbito de salud, aquellas normas generales existentes, tales como la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, el Esquema Nacional de Seguridad y el Esquema Nacional de Interoperabilidad.

b) Plan de Telemedicina 2014-2018:

En la Comunidad de Madrid, se puso en marcha el pasado mes de abril de 2014, el Plan Estratégico de Telemedicina cuyo primer fruto será un mapa de actividad de las mejores prácticas y una guía de gestión de procedimientos.

Este Plan mejorará la calidad de la asistencia sanitaria, facilitará la continuidad asistencial, aumentará la coordinación y proporcionará mejores servicios en el entorno socio-sanitario, por la reducción de barreras de acceso a los servicios.

c) Sociedad Ibérica de Telemedicina y Teleconsulta (SITT):

En el mes de marzo de 2015, se ha constituido la Sociedad Ibérica de Telemedicina y Teleconsulta (SITT) que persigue promocionar la telemedicina, y difundir sus excelencias. Esta asociación es fruto de varios años de trabajo en los que se han llevado a cabo numerosas consultas por medios no presenciales, siendo pionero en la implantación de este nuevo modelo el Servicio de TeleDermatología del Hospital Virgen de la Poveda de Madrid.

6. INFORMACIÓN Y PROTECCIÓN DE DATOS:

Con el uso de las nuevas tecnologías, la información está sometida a diversos **riesgos** por el intercambio a gran escala que se produce, y que puede llegar a comprometer la **seguridad** de la misma (puede ser alterada por el proceso de operación de los equipos, ser interceptada por entidades no autorizadas etc.), la **confidencialidad** o la **continuidad asistencial**.

6.1 Protección de los datos en salud:

La práctica totalidad de las actividades o funciones de la medicina requieren de manipulación de datos relacionados con personas identificadas o identificables. Ahondar más en materia de protección de los datos personales en el sector salud es

fundamental para **garantizar la implantación** de las nuevas tecnologías en este ámbito y para generar **confianza** en pacientes y profesionales sanitarios, si tenemos en cuenta la universalidad del tratamiento de los datos en la sociedad de la información y añadimos a esto el uso generalizado de internet y el incremento de capacidad de los teléfonos móviles.

La protección de datos es un **derecho fundamental** garantizado por el TFUE en su artículo 16, así como en la Carta de Derechos Fundamentales (artículo 7 y 8). El margen concedido a los Estados Miembros para la transposición de la Directiva 95/46/CE que contempla la protección en el ámbito del procesamiento y la libre circulación, ha provocado una gran disparidad en cuanto al nivel de protección establecido por los diferentes miembros de la Unión Europea.

Según establece la normativa vigente, se consideran **datos sensibles** los relativos al estado de salud física o mental de los pacientes (tal y como se desprende de la jurisprudencia del Tribunal de Justicia de la Unión Europea), que únicamente pueden ser objeto de tratamiento con el consentimiento expreso y escrito de su titular. Los datos sobre la salud constituyen un elemento intrínseco y primordial en la vida de una persona.

La confidencialidad de los datos adquiere en este ámbito de las nuevas tecnologías **un riesgo especial**, puesto que los datos pasan por numerosas manos, y no en todos los casos se trata de personal sanitario. En la Unión Europea, la prestación sanitaria online está basada en normas muy diversas, lo que provoca **la falta de confianza** y el desarrollo de **reticencias** para su aceptación y prestación transfronteriza por la existencia de un gran vacío legal sobre los derechos y obligaciones de las partes en lo relativo a la atención online, el consentimiento del paciente y la privacidad de los datos.

El núcleo de legislación comunitaria en materia de protección de datos lo constituye la Directiva 95/46/CE y la Decisión Marco 2008/977/JAI. Pero el alto grado de penetración en la sociedad y el elevado uso de smartphones y tablets, exige nuevos mecanismos de control y protección de los datos personales.

Por todo ello, para un buen desarrollo de la confianza del paciente y un funcionamiento eficiente de las nuevas tecnologías en salud, se hace necesaria la **reglamentación a nivel europeo de la protección de datos personales**. Esta regulación, que ya está en marcha, debe ser **específica** debido a la naturaleza y características intrínsecas de la telemedicina, ya que por una parte es servicio sanitario y por otra es servicio de la sociedad de la información.

El denominado “**paquete de protección de datos**” constará tal y como indica la Edición Española de Medical Economics de: *“un Reglamento relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y de una Directiva relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales por las autoridades competentes a efectos de la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y a la libre circulación de estos datos.”*

Para el procesamiento de la información sensible, la propuesta de Reglamento desarrollará una **protección especial** dotándoles de nuevas garantías jurídicas. Así, los datos personales de carácter sanitario deberán incluir cualquier número, símbolo o dato asignado al paciente que le identifique de manera inequívoca a efectos sanitarios, información derivada de las pruebas o los exámenes de una parte del cuerpo o sustancia corporal, incluidas muestras biológicas; así como cualquier información sobre enfermedades o riesgo de padecerlas, discapacidad, historia médica, tratamiento clínico, o estado fisiológico o biomédico real del interesado, independientemente de su fuente, como, por ejemplo, cualquier médico u otro profesional de la sanidad, hospital, dispositivo médico, o prueba diagnóstica in vitro.

6.2 Recomendaciones de la Comisión Europea:

El pasado año, la Comisión elaboró un Informe en el que destacaba la necesidad de un **blindaje de los datos sanitarios** electrónicos en España debido al déficit legislativo existente que impide la expansión de los registros de los datos sanitarios. Es clave para ello resolver los problemas relativos a la **interoperabilidad**, **acceso** y el **intercambio** de datos a nivel nacional y europeo.

Continúa el Informe haciendo referencia a la insuficiencia de los marcos institucionales, existiendo prácticas y comportamientos que se han convertido en desafíos para la implementación de la eHealth en nuestro país. Sin embargo reconoce las buenas prácticas de España en lo relativo al despliegue de los registros de datos sanitarios.

Para el desarrollo de un sistema integrado de eHealth, no solo en España sino en toda Europa, las principales barreras están vinculadas con el consentimiento del paciente. En el informe se da la posibilidad de aplicar el consentimiento para la cesión de la salud y los datos personales estableciendo determinadas restricciones y requisitos que garanticen la seguridad. Así, se entiende que una autorización o consentimiento del paciente en consulta sirve para tener acceso a la información incluso si el paciente no se encuentra de forma presencial.

6.3 Manifiesto de Valencia

El pasado 24 de marzo, la SEIS presentó un documento sobre seguridad de datos, el llamado Manifiesto de Valencia, el cual recoge los principales puntos para hacer frente a las carencias en gobierno de seguridad de la información y nuevas tecnologías en los sistemas sanitarios, así como para paliar la falta de sensibilidad y conocimiento de los profesionales en el manejo de tales datos.

El Manifiesto recoge la **autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad** como dimensiones de la calidad y seguridad de los datos y persigue la confianza digital convirtiéndose en *"un instrumento para dar confianza a los titulares de la información y a sus usuarios sobre cómo los profesionales de las TIC vamos a usar sus datos"*.

Por tanto, es necesario garantizar que la **información sensible**, no es accesible para personas no autorizadas y que los datos no puedan ser utilizados para diferentes fines de los consentidos por el paciente.

Además de la legislación vigente en la materia, se hace necesario establecer **nuevas supervisiones, orientaciones o servicios** de sanidad electrónica, e **impulsar el desarrollo de dispositivos** fiables y seguros que permitan la identificación de las personas intervinientes en el acto telemático mediante datos biométricos.

7. HISTORIA CLÍNICA:

Igual que en el uso tradicional de la medicina, a la hora de llevar a cabo cualquier consulta mediante un medio no presencial, es imprescindible llevar una correcta regulación y registro de los datos e información del paciente en su historia, dada la pluralidad de intervinientes y las complejas relaciones que pueden establecerse y derivar en diferentes responsabilidades.

Debe tenerse en cuenta que en la historia clínica, además de los **datos** se archivarán **imágenes** y que además de registrar el método utilizado para la identificación del paciente, se debe plasmar la **cantidad y la calidad** de la información recibida, así como los hallazgos, recomendaciones y servicios de telemedicina utilizados, garantizando en todo momento la **durabilidad y exactitud** de la información almacenada.

Tanto el artículo 56 de la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud, como la Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente, en su disposición adicional tercera, dirigen al Ministerio de Sanidad y Consumo el mandato de **coordinar los mecanismos de intercambio electrónico** de información clínica y salud individual, para permitir el

acceso tanto al usuario como a los profesionales en los términos estrictamente necesarios para garantizar la **calidad de la asistencia y la confidencialidad e integridad de la información**.

Todo ello exige la adopción de **elementos de interoperabilidad** entre todos los Servicios de Salud. La aplicación de criterios de normalización de la información, junto con el desarrollo de una Intranet sanitaria del Sistema Nacional de Salud, permitirá alcanzar uno de los objetivos principales del Sistema Sanitario: facilitar al máximo la **protección** de la salud de los ciudadanos en todo momento y con independencia del lugar donde precisen atención sanitaria.

Sin embargo surge en este punto una cuestión sobre la que en nuestro ordenamiento existe un vacío legal. No hay discusión sobre el hecho de que las imágenes digitales estáticas forman parte de la historia del paciente y que tal y como se desprende del artículo 17 de la Ley 41/2002, el plazo mínimo de conservación de la historia es de 5 años, plazo que algunas Comunidades como Cataluña o Navarra elevan hasta 20 años de límite. Pero las nuevas tecnologías abren nuevas formas de ejercicio de la medicina, y con ellas el uso de videoconferencias interactivas entre otros.

8. SEGURIDAD DEL PACIENTE:

Está generalmente aceptado que las nuevas tecnologías ostentan un elevado potencial de mejora en lo que a la seguridad del paciente se refiere, puesto que facilitan los procesos de adquisición, análisis y comunicación de la información, lo que hace más fácil la toma de decisiones y evita errores en su implementación

Por ello la aplicación de las nuevas tecnologías en salud juega un **papel clave** para la seguridad del paciente, al **mejorar la calidad** asistencial y cambiar el concepto de **accesibilidad**:

- Desde el punto de vista del **paciente**, al poder acceder de forma más sencilla a los facultativos,
- Desde la perspectiva del **profesional** al poder contar con segundas opiniones y mejorar la coordinación clínica y terapéutica,
- Desde el punto de vista de la **organización**, al conseguir que cada entorno asistencial disponga de la información necesaria.

El pasado mes de julio, la Sociedad de Información y Gestión Sanitaria (HIMSS), elaboró un informe que recoge aquellas aplicaciones TIC no ligadas a la Historia Clínica Electrónica, y dirigidas a 27 procesos clínicos, que tendrán un mayor crecimiento e impacto en lo que respecta a calidad y seguridad del paciente. En concreto, se refiere a aquellas herramientas dedicadas a la detección, prevención y control de infecciones nosocomiales, las enfocadas al manejo de pruebas de laboratorio, las que se centran en el análisis del estado del paciente para definir su necesidad de cuidados enfermeros, aquellas soluciones que persiguen la organización de enfermería, banco de sangre, Anatomía Patológica y servicios externalizados.

Son numerosos estudios los que aseguran como las TIC, conducen a una mayor calidad del cuidado, un aumento de la seguridad del paciente y a una mejora en la gestión del riesgo de los servicios sanitarios.

9. CORRECTA IDENTIFICACIÓN DE LAS PARTES INTERVINIENTES:

Es esencial que el profesional sanitario y el paciente se puedan **identificar mutuamente** con toda seguridad. Esta identificación será siempre necesaria cuando exista una consulta telemática, en la continuidad asistencial y para resolver cuestiones relacionadas con la responsabilidad civil y las indemnizaciones.

En muchos países, es posible el uso anónimo de la telemedicina, sin embargo el Comité Permanente de Médicos Europeos en sus recomendaciones, hace referencia a la **no permisión del uso anónimo** de la misma ni por parte de los profesionales sanitarios ni por parte del paciente, con independencia de la naturaleza (comercial o no comercial) del servicio.

Por ello es necesario que, salvo en determinadas situaciones de urgencia, médicos y pacientes dispongan de unos **elementos de identificación recíproca fiables**. Se recomienda la existencia de un reconocimiento presencial previo al uso de estas prácticas por parte del médico tele-experto mediante un examen clínico

En España existe cierto vacío legal en lo que respecta a las medidas para identificar a profesionales y pacientes en este ámbito de la medicina practicada a distancia. Como ya se ha mencionado, esta cuestión está íntimamente relacionada con la responsabilidad existente en caso de algún tipo de fallo.

La **información legal mínima** que tiene que ofrecer sobre sí mismo el prestador del servicio queda regulada en la Directiva 200/31/CE, relativa a los aspectos legales de la sociedad de la información. Así su artículo 5 establece que debe prestarse el nombre,

dirección geográfica de donde está establecido quien presta el servicio, el organismo de registro y autoridad de supervisión. Asimismo, los profesionales deberán acreditar su título profesional y el organismo y el Estado miembro en el que se encuentren colegiados.

10. RESPONSABILIDAD DE LOS PROFESIONALES INTERVINIENTES:

La identificación de la posible responsabilidad derivada de la utilización de una solución de mHealth, o de alguna forma de ejercer la medicina por un medio no presencial, sigue las normas generales pero puede ser **compleja**, debido a los **numerosos actores involucrados** en el diagnóstico, opinión, tratamiento o intervención de un caso. Se hace difícil determinar quién asume la responsabilidad cuando a la acción de como mínimo dos profesionales sanitarios, se suma la participación de profesionales de telecomunicación e informática, encargados de asegurar el adecuado mantenimiento de los equipos y del material, los fabricantes de la solución de salud móvil o el proveedor de comunicaciones electrónicas que proporciona Internet.

El **daño** a la salud del paciente puede provenir de **diversas fuentes**, lo que complica aún más su delimitación. Así puede tratarse de un dispositivo defectuoso, un diagnóstico equivocado por el profesional sanitario sobre la base de datos inexactos, un error por un especialista de nuevas tecnologías o simplemente por error del paciente al introducir o enviar los datos al profesional sanitario correspondiente.

Centrándonos en la telemedicina, podemos analizar diversos casos:

- Cuando el médico realiza una consulta de forma directa con el paciente (teleconsulta), asume la responsabilidad del diagnóstico, opinión, tratamiento e intervenciones médicas directas.
- En el caso de que participen profesionales no médicos en un acto telemédico, como por ejemplo en la recolección y transmisión de datos o en la vigilancia, el médico que corresponda debe asegurar que la formación y competencia de éstos sean adecuadas para garantizar la seguridad del paciente.
- Si se hace referencia a la televigilancia, la responsabilidad se atribuye al propio paciente, pues es quien se compromete a la recolección y transmisión de los datos al médico. Previo a esto, el médico debe comprobar que el paciente ha recibido la formación adecuada, que es capaz y que ha entendido la importancia de su papel en el proceso.

Estos son ejemplos de las complejas situaciones que pueden darse y que hacen que la **delimitación de la responsabilidad** de las personas intervinientes sea **compleja**.

11. APLICACIONES SANITARIAS (M-HEALTH):

La Sanidad móvil, según la Organización Mundial de la salud es: *“la práctica de la medicina y la prestación de servicios sanitarios mediante dispositivos móviles, como teléfonos móviles, dispositivos de seguimiento de pacientes, asistentes digitales personales (PDA, en sus siglas en inglés) y otros dispositivos inalámbricos”*

Los ciudadanos utilizan cada vez en mayor medida los dispositivos móviles para controlar su salud y poder contactar con los profesionales sanitarios. Así, tal y como indicaba en el pasado Mobile World Congress Julio Lorca, Director de Desarrollo en DKV España, en la actualidad están disponibles alrededor de 43.689 aplicaciones clasificadas en el apartado de salud y bienestar de los diferentes mercados de aplicaciones móviles. El 46% de las mismas no están en relación directa con la salud, sin embargo de las 23.682 que son consideradas sanitarias, **16.275 están orientadas a pacientes y 159 vinculadas a sensores** que registran variables cardíacas, consumo de calorías o masa corporal.

Las diferentes funcionalidades que abarcan las aplicaciones móviles permiten la recogida de diversos datos médicos, fisiológicos y relativos a la forma de vida, entorno y actividad diaria. Por ello, este tema genera numerosas dificultades y cuestiones a tratar, entre las que se encuentran:

- En primer lugar, llevar a cabo un **control** sobre las aplicaciones es muy difícil ya que hay miles y cada día aparecen nuevas.
- Las aplicaciones pueden haberse **desarrollado** en un país y que la **descarga** se realice en cualquier otro, por lo que cualquier tipo de regulación carecería de valor real.
- En tercer lugar encontramos el hecho de determinar qué entendemos por aplicación en salud y si estamos o no ante un **producto sanitario** y en consecuencia establecer quien responde ante un error de una aplicación.

El pasado año la Comisión Europea tras la publicación de su Libro Verde de la mSalud, integrado dentro del eHealth Action Plan 2012-2020, abrió una consulta pública para buscar aportaciones que ayudaran a resolver conflictos y dudas surgidas en torno al uso de dispositivos móviles en sanidad, relacionados con la protección de datos, la

seguridad del paciente, la confianza de los usuarios, la contribución de estas tecnologías a la mejora de la asistencia, y a qué nivel (Europeo, nacional o regional) deberían desarrollarse regulaciones sobre estas cuestiones.

A grandes rasgos, los principales **riesgos** a tratar son:

11.1. Propiedad intelectual:

En la elaboración y programación del software de la aplicación en concreto pueden intervenir profesionales diversos que deben **ceder los derechos** de propiedad intelectual a la entidad comercializadora de la app en concreto, por lo que se hace necesario tener bien documentada y recogida la cesión de tales derechos, así como realizar la inscripción de la misma en el Registro de la Propiedad.

Asimismo los titulares al comercializarlas están obligados a tener un **contrato de licencia de uso** con los usuarios de la app que las descargan y adquieren, de forma que queden cubiertos los principales elementos de la cesión y queden regulados otros servicios complementarios tales como la formación o el mantenimiento.

11.2. Comercio electrónico:

En numerosas ocasiones las aplicaciones **se venden**:

- De forma **indirecta**, a través de plataformas como Google Play o Apple Store lo que conlleva que se deban respetar los términos y condiciones previstos, o
- De forma **directa** a través de los sitios web de las entidades que las comercializan, que hace necesarias las correspondientes condiciones generales de contratación de forma que respeten la legislación vigente tanto en materia de servicios de la sociedad de la información y comercio electrónico como de consumidores y usuarios.

11.3. Protección de datos personales y seguridad:

Los datos están cambiando la forma de hacer negocios en el ámbito de la salud y las TICs, ya que permiten ofrecer una mayor calidad de servicios basándose en la información de los usuarios. Al ser las apps una fuente de recogida de datos y poder tratar con datos de salud, considerados como especialmente sensibles por la legislación, se hace necesaria una **estricta y minuciosa regulación** en la materia.

Es importante perseguir mejores y más fuertes herramientas de privacidad y seguridad, tales como el encriptado de los datos o mecanismos de autenticación, para fortalecer de

esta forma la **confianza** de todos los usuarios. Asimismo se debe lograr la **transparencia** de la información mediante sistemas de certificación y etiquetado de calidad para las aplicaciones móviles de estilo de vida y bienestar.

Tal y como menciona el Dictamen del Comité de las Regiones de Diciembre de 2013 sobre el Libro Verde de la Sanidad Móvil, el desarrollo de la misma debe tener en cuenta el legítimo interés de la protección de la privacidad.

11.4. Sistema de evaluación

Hay que perseguir el desarrollo de estándares y el logro de interoperatividad para las aplicaciones móviles. Las soluciones deben garantizar la seguridad de los datos personales y de las propias aplicaciones evitando virus o ataques piratas, desarrollando para ello **sistemas de evaluación fiables** como base para el desarrollo de la mHealth y que garanticen su **transparencia**.

En función de las características y funcionalidades de la aplicación, se deberá especificar el sistema de evaluación, pero tal y como indica Joan Cornet (Presidente Ejecutivo de TicSalut) en Diario Médico *“Todas necesitan que se acredite que no haya estafa, que no haya daño y que haya utilidad en clínica”*

Por todo ello, es importante la existencia de un acuerdo entre agencias evaluadoras públicas para que la acreditación de aplicaciones llevada a cabo por una, sirva para todas las demás, evitando repetir las evaluaciones por país y regiones pudiendo provocar que la aplicación llegue al mercado obsoleta.

11.5. Responsabilidad

En el uso de la mHealth, encontramos el problema de **identificar** a quien corresponde la responsabilidad potencial dado el número de agentes implicados, ya que esta por un lado el fabricante de la aplicación, además de todos los profesionales sanitarios que participen en el tratamiento y el proveedor de las comunicaciones electrónicas que suministre Internet.

El daño puede ser causado por:

- Un **dispositivo defectuoso**
- Un **diagnóstico erróneo** del profesional
- Un **fallo de la persona de IT** encargada de la aplicación
- Un **fallo del propio dispositivo** o software

- Un **uso incorrecto** del dispositivo por parte del paciente
- Envío de **datos incorrectos** al médico

11.6. Producto sanitario:

Pero la cuestión más importante ante la que nos encontramos versa en determinar qué entendemos por aplicación en salud y si estamos o no ante un producto sanitario y en consecuencia establecer quien responde ante un error de una aplicación. La normativa vigente en la actualidad no prevé regulación específica para las Apps en salud.

En el caso de ser considerada como “producto sanitario” deberá cumplir con lo indicado en la Directiva 93/42/CEE y sus modificaciones posteriores (Real Decreto 1591/2009 en España) antes de salir al mercado. Para resolver esta cuestión, la Comisión Europea publicó en 2012 una *Guía para la cualificación y clasificación del software autónomo de salud en el marco regulatorio de los dispositivos médicos*, en ella se incluye un diagrama de decisión que permite saber si una app es o no un producto sanitario mediante cuatro preguntas clave:

- ¿Es un **programa informático**?: Si la app no se ajusta a determinadas reglas de programación ni está compuesto de declaraciones e instrucciones para resolver una determinada función o tarea se trata de un documento digital y por tanto no es un dispositivo médico
- ¿**Genera o modifica datos**?: Si la aplicación únicamente se limita al almacenamiento, archivo, comunicación o compresión de los datos no se considera un producto sanitario, para ello la modificación debe tener un propósito médico.
- ¿Está pensada para **beneficiar a pacientes individuales**?: Si está enfocada a manejar datos a poblaciones o si ofrece recomendaciones genéricas no estaremos ante la definición de producto sanitario
- ¿Está **diseñada para ser usada como un producto sanitario**?: Para ello debe incorporar alguna de las siguientes funcionalidades:
 - Diagnóstico, prevención, seguimiento, tratamiento o alivio de una enfermedad

- El diagnóstico, control, tratamiento o compensación de una lesión o discapacidad
- La regulación o el apoyo de la concepción
- La exploración o modificación de un proceso o estado fisiológico
- La proporción de información para fines médicos de muestras que deriven del cuerpo humano

Por tanto, para que una aplicación sea considerada como producto sanitario deberá contestar afirmativamente a las cuatro preguntas anteriores, y si es así obtener con carácter previo a su comercialización el marcado “CE”.

11.7. Temas pendientes

Pese a los avances acaecidos en la Sanidad Móvil, todavía quedan temas pendientes tales como:

- Seguridad de las aplicaciones existentes en el mercado
- Problemas ligados a la utilización de los datos obtenidos mediante las mismas
- Falta de interoperabilidad entre las soluciones disponibles
- Desconocimiento de los requisitos legales por parte de los interesados, relativos a las normas sobre protección de datos y la obligación de obtener el marcado “CE” si tales aplicaciones se consideran dispositivos médicos.
- Favorecer y desarrollar la confianza tanto de los profesionales sanitarios, como de los propios pacientes
- Llevar a cabo una evaluación constante de las aplicaciones de mHealth, identificando la usabilidad de las aplicaciones médicas según la funcionalidad.

Es por ello que el desarrollo de aplicaciones móviles en el ámbito sanitario requiere la **adopción y puesta en marcha de medidas** que permitan garantizar la confidencialidad de los datos y la responsabilidad y persigan la protección de los datos sensibles frente a un uso indiscriminado y no autorizado, la venta ilícita de los mismos y cualquier otra forma de abuso.

Sin embargo, hay que advertir sobre los **riesgos de la sobrerregulación**, que puede obstaculizar el desarrollo de las tecnologías móviles en salud, suponiendo más trabas que beneficios.

12. ASISTENCIA SANITARIA TRANSFRONTERIZA

En 2011, el Parlamento Europeo y el Consejo promulgó la Directiva 2011/24/UE relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza que perseguía garantizar la **movilidad** de los pacientes, establecer unas reglas para **facilitar su acceso** a una asistencia sanitaria segura y de alta calidad en la Unión Europea, y promover la **cooperación** en materia de asistencia sanitaria entre los Estados miembros.

En España, el Real Decreto 81/2014 de 7 de febrero, por el que se establecen normas para garantizar la asistencia sanitaria transfronteriza, y por el que se modifica el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación, persigue definir las normas que faciliten el acceso a una asistencia sanitaria transfronteriza de alta calidad, así como promover la cooperación en materia de asistencia sanitaria entre España y los demás estados miembros.

El artículo 14 de la Directiva 2011/24/UE, establece **la red de la sanidad electrónica**, que supone un avance en lo que a la cooperación en materia de salud electrónica se refiere, y maximiza los beneficios sociales y económicos gracias a la interoperabilidad y a la aplicación de sistemas de salud electrónica.

Sin embargo, no es hasta noviembre de 2013 cuando se trazan las primeras directrices que definen los requisitos organizativos, técnicos y jurídicos necesarios para que un conjunto de datos sanitarios pueda cruzar una frontera y estén contenidos en el historial del paciente y compartidos por los profesionales sanitarios.

12.1. Problemas:

Entre los principales problemas a los que se enfrenta la salud en línea en el ámbito de la Unión Europea se encuentran la **falta de coherencia** entre las diversas políticas nacionales, la **falta de claridad jurídica** y voluntad política para la creación de soluciones y el necesario desarrollo y **mejora de la interoperabilidad** de tecnologías y sistemas.

En la prestación de asistencia sanitaria transfronteriza mediante nuevas tecnologías en la Unión Europea surgen numerosos obstáculos y riesgos para la protección de la salud al

emplear los distintos estados **formatos y normas diferentes e incompatibles**. El uso transfronterizo de implementaciones de Historia Electrónica presenta problemas de interoperabilidad jurídica, ya que los países plantean divergencias legales que pueden requerir cambios radicales en la composición técnica de la misma.

Pese a ello, es **competencia exclusiva nacional** de cada Estado Miembro la implantación de los sistemas de tecnologías de la información y la comunicación sobre la salud. De esta forma, la interoperabilidad de las soluciones de sanidad electrónica debe alcanzarse respetando las normativas nacionales sobre prestación de servicios de asistencia sanitaria.

Asimismo la creación en los pacientes de un sentimiento de **confianza** en las soluciones de eHealth es necesaria, pues solo se conseguirá su definitiva implantación si se reconocen y regulan ciertos aspectos como o la dignidad, el consentimiento, la confidencialidad y la privacidad.

12.2. Territorialidad:

Según lo previsto en la Directiva, la **asistencia sanitaria** en el caso de telemedicina se considera prestada en el **Estado donde esté establecido el prestador**, ya sea persona física o jurídica. Por ello el médico que utilice las TIC y considerado como tele-experto, deberá cumplir con los requisitos de titulación y permisos establecidos en el país en el que desempeña su actividad profesional.

13. OTROS USOS DE LAS TIC: VENTA A DISTANCIA DE MEDICAMENTOS

Los sucesivos cambios experimentados por el sector farmacéutico llevan a la aprobación del Real Decreto 870/2013 por el que se regula la **venta a distancia** del público de **medicamentos de uso humano no sujetos a prescripción médica**.

Dentro de este Decreto quedan incardinados los medicamentos de uso humano elaborados industrialmente pero no sujetos a prescripción médica, quedando excluidos aquellos sujetos a prescripción, los preparados oficinales y los medicamentos veterinarios.

Para un mayor control y seguridad, la venta por Internet únicamente podrá realizarse a través de una oficina de farmacia física y para la dispensación habrá que contar con la intervención de un farmacéutico titular.

Existe en el Real Decreto una regulación específica de las obligaciones que debe cumplir la página web, en lo relativo a **seguridad, accesibilidad, cifrado de datos**,

diferenciación inequívoca de la parafarmacia o la **prohibición de inclusión de publicidad**. Sin embargo para una completa definición de este marco regulatorio queda pendiente estar a las indicaciones de la Agencia Española del Medicamento y los organismos autonómicos que correspondan.

Por otro lado, la **Receta Electrónica** permite, mediante un sistema informatizado que el medico transmita directamente su receta a la farmacia sin necesidad de papel. Este procedimiento agiliza la información y el tratamiento posterior de las recetas a los efectos de seguimiento y facturación de las mismas.

De esta forma tanto la venta del medicamento como la receta electrónica, pese a tratarse de dos aspectos diferenciados en el ámbito sanitario deben cumplir las **medidas de seguridad y respetar los principios** consagrados en la Ley Orgánica 15/1999 de protección de datos de carácter personal, su Reglamento de Desarrollo y la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico, tanto en lo que respecta al Responsable del Fichero como a los diferentes prestadores del servicio y encargados del tratamiento que intervengan en los procesos.

Igualmente se debe asegurar que la dispensación de medicamentos no sujetos a prescripción médica se realiza con las **garantías** establecidas en el Real Decreto 870/2013 y **reforzar** las medidas de vigilancia y control para combatir la venta ilegal de productos sanitarios y medicamentos a través de Internet.

14. CONCLUSIÓN

La Unión Europea ha definido en diversas ocasiones la e-Health como el medio eficaz para lograr la **sostenibilidad** de los sistemas sanitarios, además de ofrecer la posibilidad de **mejorar** la prevención, diagnóstico, tratamiento, seguimiento y la gestión integral de la salud.

En los próximos años, además de la e-Health y la m-Health, se hablará de la T-Health o lo que es lo mismo, el servicio sanitario ofrecido a través de la televisión interactiva, en la que el usuario podrá pedir cita con su médico o acceder a canales específicos con información médica.

Esta nueva forma de ejercer la medicina, no sólo está relacionada con innovaciones tecnológicas, sino con un **cambio de la práctica diaria** en el cuidado de la salud que involucra a médicos y a unos pacientes cada vez más conectados e informados. Todo ello hace que las responsabilidades legales sean más amplias en este terreno, al suponer más riesgos porque intervienen elementos incontrolados, o muy difíciles de controlar.

Las infraestructuras TIC deben desarrollarse para el **acceso permanente** a los servicios digitales en red, tanto del profesional sanitario como de los pacientes. Por ello deben disponer de la necesaria capacidad y estar preparados para asumir el crecimiento de la demanda de servicios y la continua adaptación a la evolución tecnológica.

Se hace imprescindible el desarrollo de sistemas que permitan la **interoperabilidad y la integración de las infraestructuras** entre las organizaciones, tanto a nivel nacional como europeo y basándose en la adopción de determinados **estándares**.

Como hemos analizado en el presente trabajo, la progresiva aceptación y uso de la e-Salud depende en gran medida de la **confianza** depositada en las aplicaciones de las TIC, por ello se hace imprescindible asegurar:

- Medidas que garanticen la **seguridad de la información y la intimidad** del paciente así como la **identificación segura**, garantizando la accesibilidad, calidad y protección de los datos.
- Llevar a cabo la **sensibilización y formación** en seguridad digital entre las autoridades sanitarias, profesionales y el propio paciente
- Desarrollar procesos de **mejora continua** en lo que respecta a la veracidad, pertinencia y solvencia de la información accesible electrónicamente.
- Llevar a cabo una **estandarización terminológica**

A nivel Europeo, la Sanidad electrónica y móvil se encuentra entre las prioridades de muchos entes locales y regionales de Europa. Será necesaria una **mayor cooperación** Interregional que permita el intercambio de experiencias y mejores prácticas, de forma que aquellos que han desempeñado un papel pionero en el desarrollo de estrategias en el ámbito de las nuevas tecnologías en salud, puedan divulgar sus conocimientos.

Por todo ello se hace necesaria una **regulación homogénea de la telemedicina a nivel estatal y europeo** que lleve a un nuevo modelo de cambio asistencial, garantice la seguridad en todos los ámbitos de la esfera de los ciudadanos y haga que los profesionales sanitarios y las empresas prestadoras de este tipo de servicios gocen de un entorno favorable.

15. BIBLIOGRAFÍA:

- Ministerio de Sanidad, Servicios Sociales e Igualdad: *“La E-Salud. Prioridad estratégica para el Sistema Sanitario”*
- Saez Ayerra, Luciano: *“Infraestructuras TIC para el desarrollo de la e-Salud”*

- López Carballo, Daniel: *“La farmacia del siglo XXI, aspectos legales y nuevas tecnologías”*
- Seis: *“Telemedicina, generalidades y áreas de aplicación clínicas”*
- Pereyra Caramé, Teresa: *“mHealth: salud en tu móvil”*
- Cifuentes Ventura, Ramón: *“Riesgos jurídicos de las App en Salud”*
- Organización Médica Colegial: *“Marco legal aplicable a la telemedicina en la UE”*
- Lex Sanitaria: *“Ventajas e inconvenientes de la telemedicina”*
- Informe PWC: *“Diez temas candentes de la Sanidad Española para 2013”*
- Vítolo, Fabian: *“Telemedicina. Nuevas tecnologías- nuevos riesgos”*
- Elaboración del Plan Estratégico de Telemedicina de la Comunidad de Madrid 2014-2018
- Avellanas Chavala, Manuel: *“Los profesionales y la asistencia telemédica”*
- Furelos, Pablo: *“Europa apuesta por la eSalud para garantizar la asistencia sanitaria”*
- Fundación Orange: *“Informe e-España sobre el desarrollo de la sociedad de la información”*
- Sierra, Rosalia. Diario Médico: *“Privacidad, marco legal y seguridad, retos de la mSalud”*
- Comisión Europea: *“Libro Verde sobre Sanidad Móvil”*
- Fundación Salud 2000: *“Telemedicina: bases para la futura regulación de un mercado emergente”*
- PWC: *“Socio-economic impact of mHealth”*
- Hernández Fernández, Asunción: *“El paradigma Telemedicina vs protección de datos personales en el sector sanitario de la UE”*
- Fernández, Carmen. Diario Médico: *“Urge un marco legal para la tecnología móvil en salud”*
- Islas, Karla. Diario Médico: *“La formación de los profesionales y la evaluación, principales retos en la salud móvil”*
- Grau, Inma: *“90 años de promesas y realidades en telemedicina”*
- Sabes Figuera, Ramón: *“European Hospital Survey: Benchmarking Deployment of e-Health Services (2012–2013)”*



Centro de Estudios de
Consumo

www.uclm.es/centro/cesco

SERVICIOS Y PRODUCTOS SANITARIOS

