LOS DATOS SANITARIOS. PROTECCIÓN LEGAL. CONSIDERACIONES BIOÉTICAS.

Los datos relativos a la salud como la historia clínica están considerados como información sensible, por lo que están especialmente protegidos. Por ello, los hospitales, ambulatorios, clínicas o centros médicos están obligados a cumplir ciertas exigencias especiales en cuanto al tratamiento de la información médica de sus pacientes.

Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética (Real Decreto 1720.2007 protección de datos, art. 5.1.g). Son estos los datos que tienen su origen en la relación sanitario-paciente quien, basándose en la confianza, expone al profesional su intimidad, iniciándose así el proceso de recogida y acumulación de datos.

Principales características de las categorías de datos sanitarios electrónicos que pueden figurar en los sistemas informáticos:

1.Historial resumido del paciente	Datos sanitarios electrónicos que incluyen hechos clínicos importantes relacionados con una persona identificada y que son esenciales para prestarle una asistencia sanitaria segura y eficiente. La siguiente información forma parte de un historial resumido del paciente: 1.Datos personales 2.Información de contacto 3.Información sobre los seguros 4.Alergias 5.Alertas médicas 6.Información sobre vacunación/profilaxis, posiblemente en forma de carnet de vacunación 7.Problemas actuales, resueltos, cerrados o inactivos 8.Información textual relacionada con el historial médico 9.Productos sanitarios e implantes 10.Procedimientos 11.Estado funcional 12.Medicamentos actuales y pasados que convenga indicar 13.Observaciones sobre los antecedentes sociales relacionadas con la salud 14.Historial de embarazos 15.Datos facilitados por el paciente 16.Resultados de la observación referentes al estado de salud 17.Plan de asistencia 18.Información sobre una enfermedad rara, como detalles sobre los efectos o las características de la enfermedad
2.Receta electrónica	Datos sanitarios electrónicos que constituyen una receta de un medicamento, tal como se define en el artículo 3, letra k), de la Directiva 2011/24/UE.
3.Dispensación electrónica	Información sobre el suministro de un medicamento a una persona física por parte de una farmacia sobre la base de una receta electrónica.
4.Imagen médica e informe de imagen	Datos sanitarios electrónicos relacionados con el uso de tecnologías que se utilizan para observar el cuerpo humano con el fin de prevenir, diagnosticar, vigilar o tratar problemas de salud, o producidos por dichas tecnologías.
5.Resultados de laboratorio	Datos sanitarios electrónicos que reflejan los resultados de estudios realizados principalmente a través de diagnósticos in vitro, como la bioquímica clínica, la hematología, la medicina transfusional, la microbiología, la inmunología y otros, incluidos, en su caso, informes que corroboran la interpretación de los resultados.
6.Informe del alta médica	Datos sanitarios electrónicos relacionados con una visita médica o un episodio de asistencia sanitaria que incluyen información esencial sobre el ingreso, el tratamiento y el alta de una persona física.

En el campo de las tecnologías, el dato no es información en sí. Mientras los datos refieren a eventos o hechos registrados, la información está constituida por aquellos datos brutos que son

procesados de manera tal que generen contenido que puede ser conocido e interpretado por los usuarios.

Los datos no tienen sentido por sí mismos, pero al ser procesados y contextualizados se convierten en información certera y disponible para conocer un fenómeno, tomar decisiones o ejecutar acciones (sabiduría).

Los datos son un arma de doble filo, que pueden facilitar decisiones correctas o, por el contrario, si son mal utilizados, pueden fundamentar medidas totalmente erróneas. Los datos siempre han existido, pero ahora hay tecnología para obtener valor de ellos, siendo la base de todos los modelos de negocio.

La protección de la información ha de garantizar de los datos personales la integridad, disponibilidad, confidencialidad, cumplimiento, tratamiento según principios, etc. Para ello son necesarias implementar medidas de control en los sistemas informáticos que reduzcan los riesgos como segregación de funciones mediante perfiles de acceso, control de acceso, controles de monitorización de amenazas en red, copias de seguridad, cláusulas informativas y base legitimadora para el tratamiento de datos etc.

La gobernanza del dato o control sobre la gestión de estos datos tiene una importancia incuestionable, así como la prevención de los ataques cibernéticos.

La empresa Yahoo ha terminado admitiendo que le han robado datos de 500 millones de cuentas.

Según el informe “The State of Ransonmware in Healthcare 2022” de Sophos, en 2020 el 34% de las organizaciones de atención médica experimentaron un ataque de ransomware y en 2021 hasta casi el 66% de las organizaciones de atención médica experimentaron un ataque de ransomware.

Según datos del “Informe de Ciberpreparación 2022” de Hiscox, en 2022 el 53% de las empresas del sector sanitario y farmacéutico fue víctima de al menos un ciberataque, una cifra ligeramente superior a la media de las empresas españolas en el mismo período (51%).

La protección de la dimensión humana de los datos sanitarios, sea cual sea su tipo de almacenamiento y análisis, obliga al desarrollo de medidas jurídicas que garanticen la protección de los derechos de las personas.

En materia legal, siguen existiendo lagunas pero el Reglamento de Protección y Datos (RGPD) ha supuesto un antes y un después en la protección de datos, teniendo en cuenta la especial relevancia del dato sanitario.

Una de las obligaciones que establece el Reglamento en cuanto a la protección de datos sanitarios es la notificación de los incidentes de seguridad que se produzcan en la empresa, tanto a los afectados como a la AEPD (Agencia Española de Protección de Datos).

En el caso de que se dé una situación de ciberataque o infracción por parte de la entidad, lo ideal es estar prevenidos con un plan de respuesta ante incidentes. Se ha de notificar a las autoridades ese incidente de seguridad en un plazo máximo de 72 horas, por lo que el plan debe someterse a prueba para garantizar que cumpla con el plazo.

En nuestras leyes, la dignidad humana es el derecho que tiene cada ser humano, de ser respetado y valorado como ser individual y social, con sus características y condiciones

particulares, por el solo hecho de ser persona. Es un valor único, incondicional e inherente de todo ser humano como persona por lo que debe ser tratado siempre como un fin en sí y nunca como un simple medio para satisfacer intereses ajenos. Es un valor ético fundamental y universal. Y como tal nos obliga a seguir unos principios éticos en el manejo de los datos personales:

a) Protección: Es la obligación moral de amparar, favorecer, defender y resguardar a cualquier ser humano de un perjuicio o peligro que atente contra su dignidad y sus derechos fundamentales.
b) Confidencialidad: Es el deber de no divulgar la información personal de salud que pertenece a la intimidad de la vida de una persona. Está recogido en el deber de secreto profesional que garantiza el valor y el derecho a la intimidad.
c) Limitación de la finalidad: es la obligación de recoger y tratar estos datos sólo para los objetivos específicos y legítimos que se hayan prefijado.

Además, desde un punto de vista bioético, nuestra actuación debe basarse en:

Proteger la autonomía protegiendo la privacidad y la confidencialidad, que pueden verse amenazadas por el uso de tecnología para el tratamiento de datos. Se debe garantizar la transparencia, la accesibilidad y la inteligibilidad ofreciendo información clara, suficiente y fácilmente accesible.

Promover el bienestar y la seguridad y el interés público. Los sistemas informáticos deben satisfacer los requisitos reglamentarios de seguridad, precisión y eficacia para el tratamiento de los datos, así como establecer indicaciones bien definidas.

Fomentar la responsabilidad de su tratamiento. El tratamiento de los datos debe ceñirse a las condiciones acordadas por las partes y debe realizarse por personas debidamente capacitadas respetando siempre el fin de su uso protegiendo a las personas del daño.

Garantizar la inclusión y la equidad. El tratamiento de datos para la atención sanitaria debe diseñarse para fomentar el uso y el acceso equitativo de la forma más amplia posible, en la línea de asegurar el acceso universal a la salud.

Loreto Castilla San José y Mª Pilar Ramírez Gordo