CIRUGÍA PLÁSTICA IBERO-LATINOAMERICANA

Cir. plást. iberolatinoam.-Vol. 47 - Nº 1
Enero - Marzo 2021 / Pag. 9-12

http://dx.doi.org/10.4321/S0376-78922021000100002

PUNTO DE VISTA

Pacientes y protección de datos. Una aproximación jurídica

Patients and data protection. A legal approach

González de la Viuda M.A.

María Asunción GONZÁLEZ DE LA VIUDA
Licenciada en Derecho, Master en Derecho Sanitario.
Diplomada Universitaria en Enfermería, Instrumentista de Cirugía Plástica

Queridos lectores:

En mi doble condición de Licenciada en Derecho y enfermera instrumentista de Cirugía Plástica, he observado en distintas situaciones las dificultades que los cirujanos tienen para compaginar en su práctica diaria las nuevas tecnologías y la aplicación de una norma jurídica.

No puedo comenzar sin dar las gracias a la directora de Cirugía Plástica Ibero Latinoamericana, la Dra. Mª del Mar Vaquero, por poner a mi disposición este espacio dado que conoce mi interés por la especialidad y mi dedicación al conocimiento y difusión de las leyes que afectan a su práctica. Su ayuda y dirección han sido esenciales para llegar a buen puerto. Y como parte de ese interés, les hago llegar estas reflexiones sobre la protección de datos personales, entendida como la salvaguarda del conjunto de datos de una persona sobre su uso y destino, frente al uso de la informática para garantizar su honor e intimidad.

Cuando estas líneas vean la luz ya se habrán cumplido dos años desde que entró en vigor el Reglamento General de Protección de Datos de la Unión Europea, que tiene como objeto fortalecer y unificar la protección de datos en el marco de la Unión Europea. Una de las razones por las que ha tenido una enorme repercusión, a mi juicio, es la cuantía tan elevada de las sanciones económicas, de hasta un cuatro por ciento de las ganancias anuales de la empresa, así como también el riesgo en su reputación.

A lo largo de nuestra vida todos somos o seremos usuarios del sistema sanitario; es decir, nuestros datos más sensibles, los de salud, van a ser tratados por médicos, sanitarios, centros de salud y hospitales, tanto en la sanidad pública como en la privada, y en esta última además estos datos pueden incluir datos bancarios, así como sociosanitarios, personas de apoyo, etc.

Si nos referimos a la especialidad de Cirugía Plástica, Estética y Reparadora, los datos además se complementan con fotos, diagramas o esquemas, que en muchos casos y hasta no hace demasiado tiempo, se encontraban en carpetas de papel, y que ahora, en muchos casos, viajan por los nodos de la red para encontrar una segunda opinión. Para ambos casos, y pensado desde la doble vertiente de pacientes y sanitarios dedicados a la Cirugía Plástica, intentaremos con este artículo abrir el camino para que nuestros pacientes se encuentren seguros.

Imaginemos por un momento las circunstancias actuales, durante la situación epidemiológica de la infección por coronavirus SARS-CoV-2, muchas de las consultas que antes se realizaban de forma presencial han pasado a lo que se conoce como teleconsultas, que en épocas anteriores a la pandemia eran meramente anecdóticas. La pregunta que nos corresponde hacer es ¿se ha preguntado al paciente?, ¿este ha consentido en que se celebre así? Incluso quizá antes el profesional médico debería preguntarse ¿estoy usando como cirujano una red segura? Entiendan como segura el uso de un sistema de comunicación encriptado en el que la información se transforma de forma que solamente la entiendan el emisor y el receptor, para que si por cualquier causa cae en manos de terceros, el paciente sea difícilmente identificable.

Poco podemos añadir al tema que rige la teleconsulta; solo remitirles al artículo que esta misma revista publicó en su número anterior (número 4 de 2020) firmado por Ofelia de Lorenzo, letrada y Vicepresidenta Primera de la Asociación Española de Derecho Sanitario.[1]

Los datos de salud tienen un alto valor, por lo que hay que prevenir que aprovechando la incertidumbre que provoca el contexto actual, se produzcan abusos por parte de terceros que conduzcan a situaciones de pérdida de libertades, discriminación u otros daños en la situación personal de los ciudadanos. En esta situación, es preciso que conozcamos distintas normas jurídicas que nos son de aplicación, tanto como pacientes, como médicos garantes de su protección.

La primera norma aplicable en España, es el Reglamento Europeo de Protección de Datos (SP/LEG/19835) -Reglamento (UE) 2016/679- y es una norma directamente aplicable que requirió incluso la sustitución de la Ley Orgánica 15/99 de Protección de Datos (LOPD). Esta nueva ley se denomina Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGD). Creo importante destacar en esta nomenclatura la idea de que se denomina Orgánica, lo que para los profesionales médicos significa que estamos protegiendo un Derecho Fundamental invocable por parte de cualquier persona frente a una actuación médica realizada tanto en la actividad pública como en la privada.

¿A qué se refiere la terminología protección de datos en el ámbito de la salud? A todos aquellos datos que el paciente se ve obligado a trasladar a la documentación sanitaria. Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable, y para determinar si una persona física es identificable deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. A su vez, para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.

En estos registros (documentación clínica), cualquiera que sea su formato, les corresponde a sus responsables la observancia de la normativa de protección de datos. Por ello, deberán cumplir con obligaciones como la de informar sobre las condiciones del tratamiento (finalidad, plazos de conservación, destinatarios de los datos…), minimizar el número de datos personales tratando los estrictamente necesarios o limitar la finalidad del tratamiento, de tal forma que los datos sean recogidos con fines determinados, explícitos y legítimos. Igualmente, en caso de un posible tratamiento ulterior de los datos con fines distintos – presentación a congresos-, este solo se debe producir si existe compatibilidad con los fines de su recogida inicial, informando en todo caso a los interesados de ese nuevo fin.

En España, refiriéndonos a la sanidad pública, está garantizado su cumplimiento y las Comunidades Autónomas disponen en sus organizaciones de oficinas de seguridad que tienen como objetivo velar por un adecuado grado de madurez de la seguridad de los sistemas de información en los hospitales y centros de salud que aseguren la continuidad del servicio y otros riesgos, como perdida de datos o confidencialidad. Ahora bien, la normativa, no hace distinciones sobre si el paciente es tratado en un hospital público o en la consulta privada de un facultativo. Por tanto es necesario no solo conocer, sino cumplir la normativa.

A nivel nacional disponemos de la Agencia Española de Protección de Datos (AEPD), que es la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de los ciudadanos. Su objetivo es, por un lado, fomentar que los ciudadanos conozcan sus derechos y las posibilidades que la Agencia les ofrece para ejercerlos; y por otro, que los sujetos obligados tengan a su disposición un instrumento ágil que les facilite el cumplimiento de la normativa. Este proceso se basa en la asesoría y el seguimiento de la normativa aplicable, así como en estándares y códigos de buenas prácticas relacionados con la seguridad de los sistemas de información.

Teniendo en cuenta lo dicho, no es recomendable almacenar información de pacientes en teléfonos móviles u ordenadores portátiles. Lo mismo que tampoco es recomendable usar las aplicaciones de mensajería telefónica. Para el primer caso se recomienda proteger el dispositivo con códigos seguros, incluso utilizar uno diferente al personal y para el otro conocer las condiciones de privacidad y uso. En el caso de estar trabajando en un centro público, los accesos a la documentación así como su cumplimentación queda registrada y su trazabilidad garantizada. Además, de manera aleatoria se realizan auditorías internas. La ley obliga a tener la misma diligencia en el caso de una actividad privada, por lo tanto también es de obligado cumplimiento en cada una de las consultas.

Algunas novedades jurídicas que es imprescindible conocer:

1- El consentimiento del paciente para que sus datos sean tratados ha de ser inequívoco. Es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa. No es válido, como lo era antes, que el paciente no hubiera expresado su opinión, sino que ahora es imprescindible que asienta. Para ello, en la historia clínica debe quedar reflejado y lo que habitualmente se hace es que, junto al documento que firma para consentir una consulta o una intervención quirúrgica (consentimiento informado), se le pregunte además por el tratamiento de sus datos y manifieste que consiente en que estos sean tratados.
2- La información a los interesados, tanto respecto a las condiciones del tratamiento de sus datos como en las respuestas al ejercicio de sus derechos, deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

Uno de los derechos que asiste a los pacientes es el derecho de rectificación de sus datos, al que se refiere de este modo el reglamento y la propia ley, "Derecho de rectificación: el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional" (Art. 16 del Reglamento). En la solicitud, el paciente deberá indicar a qué datos se refiere y la corrección que hay que realizar. Además, cuando sea necesario, deberá acompañar la solicitud de la documentación que justifique la inexactitud o el carácter incompleto de sus datos.

¿Quiere esto decir que un paciente puede pedir que eliminemos de su historia clínica algún dato? Cuando el dato que se pretenda rectificar, que ha de constar en la historia y a juicio del facultativo ha de ser pertinente y veraz, tenga la consideración de imprescindible para la prestación de una adecuada asistencia sanitaria, no será "eliminable". Igualmente, a modo de ejemplo en los tribunales españoles, cuando un paciente ejercitando este derecho ha pretendido que se omitiera de su historia clínica por ejemplo una antigua adicción, encontramos que habiendo entendido el tribunal que ese dato era necesario para el tratamiento, ordenó que permaneciera en la documentación.

No podemos olvidar que en ocasiones, con motivo del ingreso hospitalario de pacientes que podemos llamar "conocidos", se produce un número elevado de accesos a su historial clínico. Esos accesos solo se consideran legítimos cuando se producen por necesidades asistenciales; si no es así, con este mero acceso no solo vulneramos la normativa de protección de datos, sino que puede ser considerado como un delito que en el caso de España se encuentra tipificado en el código penal como descubrimiento y revelación de secreto.

Antes de finalizar y dado el carácter iberoamericano de esta revista, les apunto unas breves ideas. El reglamento europeo, desde su aprobación, ha tenido un efecto contagio en Latinoamérica donde se observa un aumento del dinamismo en la creación de empresas tecnológicas, con fórmulas para formar y coordinar acciones que aumenten las infraestructuras digitales y garanticen la privacidad y la protección de datos. Pero sin embargo, a estas alturas, no existe una normativa común, ni siquiera unanimidad en la creación o gestión del organismo que tutela este derecho.

Solo me queda ya acabar este escrito con unas líneas que les sean útiles en la práctica diaria:

Los consentimientos para las actuaciones médicas no deben ser confundidos con las bases jurídicas para los correspondientes consentimientos de tratamientos de datos.

La privacidad de los pacientes, el secreto y la seguridad de sus datos han de ser garantizados, por ello adoptaremos las medidas técnicas y organizativas necesarias para evitar su pérdida, mal uso, alteración y robo.

El acceso a la información del paciente se limita a aquellos que la necesiten para atenderle en los procedimientos que necesiten. Deben regularse los niveles de acceso según los perfiles de cada profesión, así como garantizar la trazabilidad de los accesos a la historia clínica con códigos seguros, únicos y personales, y nunca utilizando usuarios genéricos. En el caso de usar documentación en papel, deben establecerse mecanismos para comprobar su integridad y custodia.

Puede ser interesante, además, la firma de un compromiso de confidencialidad durante el tiempo que se presten servicios o de una manera indefinida.

Utilicen la seudonimización, es decir, el tratamiento de datos de manera tal que no puedan atribuirse a un interesado sin utilizar información adicional; dicha información debe figurar por separado y estar custodiada para certificar que esos datos se atribuyen a una persona física.

Hay que evitar utilizar aplicaciones y soluciones de teleconsulta que no ofrezcan garantías y que puedan dar lugar a la exposición de los datos personales del paciente a través de los servicios de correo y mensajería.

Recurran a proveedores y encargados que ofrezcan soluciones probadas y garantías suficientes. Si estos acceden a datos de carácter personal, tendrán la consideración de encargados de tratamiento y la relación se regirá por un contrato u otro acto jurídico que vincule al encargado respecto del responsable. Este contrato debe establecer el objeto, la duración, la naturaleza y la finalidad del tratamiento de los datos, el tipo de datos personales y categorías de interesados, así como las obligaciones y derechos del responsable.

mgonzalez685@hotmail.com

Bibliografía

1. **De Lorenzo Aparici, O.** Telemedicina: ética y responsabilidad. *Cir. plást. iberolatinoam.* 2020;*46*(4): 379-380.

Legislación consultada

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (referenciada en el artículo como LOPD o antigua LOPD).

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.