CIRUGÍA ESPAÑOLA

www.elsevier.es/cirugia

Artículo especial

Guía práctica para el uso de registros visuales en la era del Reglamento General de Protección de Datos de la Unión Europea

Luca Ponchietti[a,*], *Nuno Filipe Muralha Antunes*[b], *Alejandra Utrilla Fornals*[a], *Peep Talving*[c], *Alessandro Garcea*[d], *Marta Roldón Golet*[c], *Melody García Dominguez*[c] y *Carlos Yanez Benitez*[e]

[a] *Servicio de Cirugía General, Hospital Universitario San Jorge, Huesca, España*
[b] *Department of Surgery, Centro Hospitalar do Médio Ave, Santo Tirso, Portugal*
[c] *Department of Surgery, North Estonia Medical Center, University of Tartu, Tartu, Estonia*
[d] *Servicio de Cirugía General, Hospital Universitario de Elche, Elche, España*
[e] *Servicio de Cirugía General, Hospital Royo Villanova, Zaragoza, España*

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:
Recibido el 23 de junio de 2020
Aceptado el 20 de septiembre de 2020
On-line el 27 de octubre de 2020

Palabras clave:
Reglamento General de Protección de Datos de la Unión Europea
Unión Europea
Ley de Protección de Datos
Registros visuales
Anonimización
Almacenamiento de datos

RESUMEN

El nuevo Reglamento General de Protección de Datos de la Unión Europea (más comúnmente conocido por sus siglas en inglés como «GDPR») conforma un nuevo marco para la protección de datos común para la Unión Europea. Es por ello que los profesionales del ámbito sanitario deben revisar cómo recopilan y comparten datos para garantizar que estos cumplan con todos los estándares.

El propósito de este artículo es concienciar sobre el Reglamento General de Protección de Datos de la Unión Europea y proporcionar una guía práctica que ayude a evitar problemas legales en la redacción de artículos o la preparación de comunicaciones científicas que requieran compartir datos personales y visuales.

Para hacer esto, se han analizado las más comunes situaciones donde es necesario recoger y utilizar datos personales y visuales, para finalmente dar una serie de respuestas y recomendaciones para todos los escenarios descritos.

Use of visual media in the era of European Union's General Data Protection Regulation: A practice-oriented guideline

Keywords:
European Union's General Data Protection Regulation

ABSTRACT

With the European Union's new General Data Protection Regulation, commonly known as ''GDPR'', as the new framework for data protection across the European Union, doctors will need to review how they collect and share personal data to ensure they meet the standards.

* *Autor para correspondencia.*
Correo electrónico: lponchietti@salud.aragon.es (L. Ponchietti).

https://doi.org/10.1016/j.ciresp.2020.09.005

European Union
Data Protection Law
Visual media
Anonymisation
Data storage

The aim of this article is to raise awareness on the General Data Protection Regulation, and to provide an easy guideline to steer free from legal problems at the time of drafting papers, presenting lectures and sharing personal data and visual media in particular.

To do so, we have analysed the most common situations where personal data, and above all visual media, can be collected, giving clear-cut answers and recommendations for all the scenarios.

Introducción

El personal sanitario tiene el privilegio de acceder a la información personal y confidencial de los pacientes. Esta información puede variar desde temas aparentemente irrelevantes como el estilo de vida, la edad de la pubertad, etc., hasta aspectos más íntimos como la orientación sexual, el padecimiento de enfermedades transmisibles o el consumo de drogas. Los profesionales de la salud en general y los médicos en particular han sido históricamente considerados competentes para mantener en secreto los datos confidenciales. Es por ello que los pacientes suelen sentir la suficiente seguridad para responder cualquier pregunta y proporcionar cualquier información personal porque asumen que estarán en un ambiente de confianza con sus médicos. El mismo nivel de confianza se encuentra, también, implícitamente reconocido y es esperable por parte de cualquier institución sanitaria.

Desafortunadamente, con la aplicación oficial del nuevo reglamento de protección de datos, parece poderse afirmar que lo que los profesionales sanitarios consideran como datos confidenciales ya no lo son tanto. A menudo los médicos están ocupados lidiando con desafíos clínicos, aunque frecuentemente estén a su vez llamados a resolver todos los demás asuntos relacionados con la práctica médica.

Las sociedades científicas y los consejos médicos no han subrayado la relevancia de la protección de datos fuera de las consideraciones más básicas. La información confidencial se comparte habitualmente sin cumplir con las reglas vigentes para proteger tales datos, y aunque los profesionales de la salud entiendan y respeten los principios de confidencialidad, a menudo carecen de la capacidad para discernir qué son considerados datos sensibles. En la actualidad es muy común tomar fotografías o vídeos mediante telefonía móvil para posteriormente compartirlos a través de servicios de mensajería instantánea (como WhatsApp, entre otros) o mediante la asistencia a congresos médicos o la lectura de documentos científicos, en los que los mismos datos se comparten libremente. La creencia más común en la práctica médica es que «siempre que no se pueda reconocer al paciente, el uso de sus imágenes o vídeos está permitido». Pero esta es una simplificación excesiva que no va en la línea de la legislación vigente.

En este artículo se analiza el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, el denominado Reglamento General de Protección de Datos de la Unión Europea (UE), comúnmente conocido como GDPR por sus siglas en inglés para *General Data Protection Reglament,* que perfila el marco para la protección de datos en toda Europa. Este documento se firmó el 27 de abril de 2016 y entró en vigor el 25 de mayo de 2018[1].

Los países que forman la UE han creado organismos nacionales responsables de proteger los datos personales de conformidad con el artículo 8 (3) de la Carta de los Derechos Fundamentales de la UE. La aplicación coherente de las normas de protección de datos en toda la UE se encuentra garantizada por el Comité Europeo de Protección de Datos, que es un organismo europeo independiente, compuesto por representantes de las autoridades nacionales de protección de datos de los países de la UE y del Supervisor Europeo de Protección de Datos.

Es importante tener en cuenta el hecho de que el GDPR protege a cualquier individuo vivo que resida en la UE, sea ciudadano de la UE o extranjero. Por ello, el GDPR no es aplicable si el interesado ha fallecido o en el caso de que los datos correspondan a ciudadanos de la UE que residan en un país no perteneciente a la UE. Además, el GDPR no regula los casos en que el procesamiento de datos sea realizado por una persona para fines ajenos a su oficio, negocio o profesión.

El GDPR destaca las necesidades de transparencia con los interesados y de un propósito legítimo para el procesamiento de datos personales. También define los datos personales como cualquier información de un natural identificable como persona o «sujeto de datos». Además, destaca que los datos deben ser limitados y relevantes para un propósito específico, que debe declararse a los sujetos interesados, los cuales deben dar su consentimiento explícito. Otros pilares del GDPR son el almacenamiento de datos, la necesidad de borrar datos cuando ya no sean útiles (el denominado «derecho a ser olvidado») y la gobernanza de los datos en su conjunto.

Según el GDPR, la obtención de datos personales ya implica, por definición, el procesamiento de los mismos, de tal forma que se entiende por «procesamiento» cualquier operación realizada sobre los datos personales. Los ejemplos de procesamiento según el GDPR son: la recopilación, grabación, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión, puesta a disposición, alineación o combinación, restricción, borrado o destrucción.

De forma práctica, en lo que se refiere a los pacientes, los datos personales son cualquier tipo de información que permita o pueda permitir su identificación. El GDPR entra en juego cuando estos datos personales son recopilados y

procesados por parte de un tercero (personas físicas o entidades legales).

El GDPR también define las figuras de «responsable del tratamiento de los datos» (*controller* en idioma inglés) y de «encargado del tratamiento de los datos» (*processor* en idioma inglés), que desempeñan diferentes roles en la gestión de datos personales. El responsable determina los propósitos y medios para el procesamiento de datos personales, mientras que el encargado maneja los datos personales en nombre del responsable. Por tanto, el responsable se encuentra jerárquicamente en una posición superior, lo que conlleva más responsabilidades. Ambos pueden ser personas físicas, autoridades públicas u otros organismos.

En ciertos casos, cuando se requiera un seguimiento regular y sistemático de datos a gran escala, un delegado de protección de datos debe ser designado por parte del responsable y del encargado. Sus funciones son informar y asesorar tanto a los anteriores como a sus delegados sobre su obligación de cumplir con el GDPR y otras leyes de protección de datos de ámbito nacional, así como supervisar su cumplimento mediante auditorías.

Dada la gran amplitud de alcance del GDPR, se ha decidido centrar la atención solo en sus implicaciones para el uso de datos de pacientes. Principalmente sobre cómo deben usarse o compartirse adecuadamente los medios visuales (pruebas de imagen, fotografías y vídeos) y qué limitaciones deben tenerse en cuenta en la práctica habitual.

El objetivo es proporcionar una guía práctica que ayude a evitar problemas legales en la redacción de documentos, la preparación de comunicaciones científicas o a la hora de compartir imágenes o vídeos con compañeros del ámbito sanitario.

Métodos

Un grupo de estudio del Comité Educativo de la Sociedad Europea de Trauma y Cirugía de Emergencias se formó en 2019 con el objetivo de evaluar los requisitos que los médicos deben cumplir de acuerdo con el GDPR, no solo para el manejo de datos personales, sino principalmente para la utilización de medios visuales. Para hacerlo, utilizamos un proceso Delphi modificado *ad hoc*, donde los autores del artículo eran los mismos receptores de los cuestionarios Delphi.

Como primer paso, los autores plantearon la hipótesis de una serie de escenarios en los que era necesario recopilar y utilizar datos personales para medios visuales, o situaciones en las que podrían surgir problemas relacionados con su uso. Todos los escenarios se basan en situaciones comunes en las que el médico es un empleado de un hospital público o privado. El número total de escenarios acordados fue de 24. A continuación, todos los autores revisaron y estudiaron de forma detallada el documento de GDPR.

Una vez realizado esto, cada autor respondió de manera independiente a los 24 escenarios, con un enfoque de respuesta concisa, según las recomendaciones legales y de práctica clínica. Por último, las respuestas fueron revisadas y discutidas por todo el grupo, durante 2 videoconferencias en directo, hasta que todos los escenarios fueron resueltos con la conformidad de todos los autores.

Guías

1. ¿Se pueden obtener registros visuales sin consentimiento explícito, con fines clínicos y solo en interés del paciente?

Respuesta: Sí, en determinados supuestos. Los profesionales de la salud pueden procesar (grabar, almacenar, reproducir, etc.) registros visuales sin consentimiento explícito, siempre que se haga en el mejor interés del paciente.

Antecedentes: El artículo 9 del GDPR establece una serie de situaciones en las que el procesamiento de datos pertenecientes a «categorías especiales», como pueden ser las relacionadas con la salud, puede llevarse a cabo de manera legal. A la práctica médica se aplica el párrafo 2 (c, d, i, h), que permite el procesamiento de datos personales si se lleva a cabo para interés del paciente, de salud pública, con fines diagnósticos o de mejoría de la calidad y la seguridad asistenciales, entre otros[1].

Recomendación: Es aconsejable obtener el consentimiento del interesado para procesar los registros visuales antes de llevar tal acción a cabo. No obstante, aunque no se haya obtenido con anterioridad el consentimiento, pero se considere de interés para el paciente la obtención de registros visuales de un procedimiento/hallazgo, estos podrán ser obtenidos.

2. ¿Se pueden compartir los registros visuales a través de mensajería instantánea o correo electrónico con fines clínicos?

Respuesta: Sí. Pero solo mientras se haga con un propósito clínico y se respete la integridad y confidencialidad del paciente.

Antecedentes: La información personal del paciente que se obtenga legalmente (ver el artículo 9 del GDPR) puede ser compartida siempre que se haga de acuerdo con el artículo 5 del reglamento. El citado artículo engloba los principios del procesamiento de datos y, con respecto a nuestro ejemplo, en el párrafo 1 (h) se establece que: Los datos personales se «procesarán de una manera que garantice su seguridad adecuada, incluyendo su protección contra otro tipo de procesamiento no autorizado o ilegal y contra pérdida accidental, destrucción o daño de los mismos, utilizando las medidas técnicas u organizativas que se consideren apropiadas (''integridad y confidencialidad'')»[1].

Recomendación: Cada institución sanitaria debe proporcionar políticas claras sobre el intercambio de archivos visuales, identificando el modo correcto para hacerlo y asegurando que se mantenga la confidencialidad del paciente en todo momento. Por esta razón, y debido a la definición imprecisa de «seguridad apropiada» de los datos personales en el GDPR, si no se han establecido las políticas de protección pertinentes, compartir imágenes o vídeos con compañeros del ámbito sanitario, usando aplicaciones de mensajería instantánea o correo electrónico, incluso si están protegidos por varios grados de seguridad (codificación, cifrado o identificación biométrica), no puede considerarse conforme con el GDPR y, en nuestra opinión, no debería hacerse. Si los registros visuales necesitan ser compartidos, su institución (como

figura de *responsable*) debe proporcionar los medios para hacerlo.

3. ¿Cómo deben almacenarse los registros visuales y por cuánto tiempo?

Respuesta: Si no están anonimizados, los datos personales deberían ser almacenados bajo un nivel de seguridad apropiado, según el riesgo de filtración, y no mantenerse durante más tiempo del estrictamente necesario.

Antecedentes: En virtud del artículo 32, las figuras de *responsable* y *encargado* de los datos garantizarán que la seguridad de estos sea proporcional al riesgo de su destrucción accidental o ilegal, a su pérdida, alteración, divulgación no autorizada o al acceso a datos personales transmitidos, almacenados o procesados de otra manera. Para hacerlo, se pueden utilizar diferentes técnicas (encriptación, seudonimización, etc.)[1].

Recomendación: Es aconsejable anonimizar los registros visuales. Si no son de carácter anónimo, se debe comprobar el nivel de seguridad y elegir una forma adecuada de almacenar los mismos. De forma práctica, se recomienda no mantener los registros visuales en su teléfono móvil personal, ordenador o unidades externas. De no ser así, al menos se debe usar un servicio de encriptación potente. La solución más segura es que cada institución sanitaria (actuando en figura de responsable) establezca dónde y cómo almacenar los datos visuales no anonimizados, de manera que se libere de esta responsabilidad al personal sanitario.

4. ¿Se pueden utilizar registros visuales obtenidos con fines clínicos para finalidades no clínicas (como comunicaciones a congresos, redacción de documentos, enseñanza, etc.)?

Respuesta: Sí, si se ha obtenido el consentimiento para ello. Sí, bajo requerimiento judicial. Sí, si se trata de datos anonimizados.

Antecedentes: El artículo 9 establece la posibilidad de utilización de datos personales si se solicita un consentimiento explícito para ello. Además, se pueden compartir datos personales en circunstancias bajo requerimientos legales. Finalmente, si los datos son completamente anónimos, el GDPR no es aplicable[1].

Recomendación: Aunque la anonimización es una herramienta valiosa y es aconsejable usarla siempre que sea posible, es conveniente contar con el consentimiento de los pacientes antes de utilizar registros visuales para ámbitos no clínicos. También es recomendable contar con el consentimiento del paciente para la anonimización de datos visuales. Desde una perspectiva práctica, deberían establecerse estrategias para anonimizar los registros visuales y hacer que sean revisadas y aceptadas a nivel institucional. En este sentido, y como posteriormente se explicará, es fundamental no confundir la anonimización con la seudonimización de los datos.

5. ¿Se pueden utilizar registros visuales «antiguos», obtenidos antes de la entrada en vigor del GDPR?

Respuesta: Sí, si el paciente ha fallecido. Sí, en el caso de que ya se encuentren anonimizados. Sí, si se obtiene un consentimiento específico.

Antecedentes: El GDPR no incluye excepciones que permitan el uso de los datos recopilados anteriormente a su entrada en vigor y que no cumplan sus normas. A partir del 25/05/2018, fecha de entrada en vigor del GDPR, quedó derogada la Directiva 95/46/CE anterior[1].

Recomendación: Se aconseja confirmar que todos los registros visuales que se estén utilizando cumplan con la normativa GDPR. En el caso de que se consideren históricos o «antiguos», es necesario cerciorarse de que no haya forma de reconocer la identidad del sujeto de los datos (anonimización) o que el marco de tiempo le asegure que los pacientes ya fallecieron.

6. ¿Se pueden utilizar registros visuales sin fines clínicos si no se ha obtenido previamente el consentimiento del paciente?

Respuesta: Sí, si los registros visuales se han obtenido legalmente y ni usted ni el público pueden reconocer al paciente (anonimización).

Antecedentes: El artículo 9 del GDPR establece una serie de situaciones consideradas dentro de «categorías especiales», tales como las relacionadas con la salud, que permiten el procesamiento de datos personales de manera legal. Como ya hemos mencionado, el párrafo 2 (c, d, i, h) es aplicable a la práctica médica, por lo que el procesamiento de datos personales queda permitido si se lleva a cabo para interés del paciente, de salud pública, con fines diagnósticos o de mejoría de la calidad y seguridad asistenciales. La anonimización es una forma de procesamiento y, una vez anonimizados, los datos personales dejan de regularse bajo la normativa GDPR[1,2].

Recomendación: Es mejor contar con el consentimiento del paciente para el uso de registros visuales y se recomienda obtenerlo siempre que sea posible. En algunos casos, sin embargo, no es práctico o no es posible, como, por ejemplo, si se trata de pacientes que viven en otros países de la UE, casos de enfermedades cognitivas degenerativas, etc. Si los datos se obtuvieron legalmente de acuerdo con el GDPR y se anonimizaron, pueden ser utilizados.

7. ¿Se pueden anonimizar/seudonimizar los registros visuales sin el consentimiento del paciente?

Respuesta: Probablemente sí.

Antecedentes: La anonimización y la seudonimización son 2 formas de procesamiento de datos. Por un lado, la normativa GDPR afirma en los artículos 5 a 9 y 12 a 14 que para procesar datos legalmente es necesario contar con el consentimiento del interesado (en nuestro ámbito, el paciente). Por lo tanto, el profesional sanitario debe informar al paciente de que uno de los propósitos de la recopilación de sus datos es anonimizarlos/seudonimizarlos para su uso futuro. Si esto no se ha hecho, la anonimización/seudonimización de los datos personales puede considerarse un «procesamiento posterior» más allá de los fines para los que se otorgó inicialmente el consentimiento, lo cual está sujeto a una serie de limitaciones bajo la normativa GDPR. Por otro lado, de acuerdo con el artículo 9, se podría argumentar que se contemplan una serie de circunstancias en las que se pueden obtener datos personales sin consentimiento explícito, por ejemplo, si es

útil para fines médicos diagnósticos. En este supuesto, se puede considerar que los datos personales se habrían obtenido legalmente, admitiendo cualquier forma de procesamiento permitido, entre los que está la anonimización/seudonimización, con el objetivo final de cumplir con la normativa GDPR[1].

Recomendación: El GDPR es extremadamente complejo y muchos detalles técnicos no son sencillos de interpretar, por lo que en esta ocasión no se puede responder de manera contundente. Según lo expuesto en este documento, para utilizar registros visuales con fines educativos médicos (congresos, artículos, conferencias, etc.) se considera que lo más adecuado es recomendar, si se encuentra en posesión de estos datos, obtener el consentimiento pertinente de acuerdo con la regulación del GDPR. Por otro lado, si el paciente consintió en el pasado la recogida de los mismos, se podrían anonimizar/seudonimizar dentro de la legalidad, de acuerdo con las consideraciones expuestas en el artículo 9. Sin embargo, es necesario puntualizar que probablemente sea ilegal acceder a los datos personales del paciente de forma posterior y anonimizarlos/seudonimizarlos (por ejemplo, tras el alta del paciente) si en su momento no se obtuvo el consentimiento para ello.

8. ¿Cómo se pueden anonimizar los registros visuales?

Respuesta: La anonimización se puede lograr a través de diferentes técnicas, todas ellas con el objetivo común del eliminado de identificadores personales directos e indirectos.

Antecedentes: La anonimización es el proceso de eliminar identificadores personales tanto directos (nombre, fecha de nacimiento, número de la Seguridad Social, etc.) como indirectos (vincular información con otras fuentes, metadatos, ejemplos como enfermedades raras, tatuajes únicos, etc.) que pueden conducir a la identificación de un individuo. El artículo número 26 del GDPR establece que, al determinar si un individuo es identificable o no, deben tenerse en cuenta todos los medios razonablemente susceptibles de ser utilizados, ya sea por la figura del controlador o por otra persona, para identificar a la persona física directa o indirectamente. Por ello se deben tener en cuenta todos los factores objetivos, como los costes devenidos y la cantidad de tiempo requerido para su identificación, teniendo en cuenta el desarrollo tecnológico en el momento del procesamiento de los datos, para determinar si los datos personales se convirtieron correctamente en anónimos, así como qué medios podrían ser necesarios para reidentificar al sujeto de los datos. Un proceso de anonimización puede considerarse válido si se puede demostrar que se torna en poco probable la identificación del sujeto de datos, dadas las circunstancias del caso individual y el estado de la tecnología. Con respecto a los registros visuales, es importante tener en cuenta que tanto el responsable como el encargado aún pueden estar en condiciones de volver a identificar a los pacientes después del anonimato debido a la recogida directa de sus datos personales o de circunstancias particulares. En tales casos, los datos aún deben considerarse datos personales mientras estén en manos del responsable/encargado[1,2].

Recomendación: La anonimización es un procedimiento delicado. De acuerdo con el archivo audiovisual que se desea anonimizar, conviene evaluar qué métodos deben usarse teniendo en cuenta todos los posibles riesgos para la identificación del paciente (singularización, enlace de datos, inferencias) y la probabilidad de tener un «intruso» (individuos que pueden identificar intencional o inadvertidamente al sujeto de datos). El responsable debe abordar estos problemas y dotar al encargado de los medios para llevar a cabo el anonimato. Se recomienda obtener y seguir solo procedimientos aprobados por cada institución, para evitar responsabilidades personales.

9. ¿Se pueden utilizar registros visuales anónimos?

Respuesta: Sí.

Antecedentes: Los datos personales anónimos no se encuentran sujetos a la regulación GDPR[1].

Recomendación: Según el GDPR, se pueden utilizar registros visuales anónimos. Sin embargo, se recomienda comprobar que no existe otra legislación a nivel institucional o local que prohíba su uso.

10. ¿Cómo se pueden seudonimizar los registros visuales?

Respuesta: Hay muchas formas de seudonimizar datos y todas ellas tienen en común el acto de cambiar los datos originales por seudónimos. Este proceso a veces se denomina enmascaramiento de datos y se puede lograr de diferentes maneras, tales como sustitución, barajado, varianza de números y fechas, cifrado, anulación o eliminación, etc.

Antecedentes: El artículo 4 establece que la «seudonimización» consiste en el «procesamiento de datos personales de tal forma que dichos datos personales ya no se puedan atribuir al interesado sin utilizar información adicional, siempre que dicha información se mantenga por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable»[1–3].

Recomendación: La seudonimización no debe considerarse un medio eficaz de anonimización, pero puede considerarse una medida para mejorar la seguridad y minimizar el riesgo de vinculación entre un conjunto de datos. Los datos seudonimizados todavía se encuentran bajo la regulación GDPR. Por todo ello, la figura del responsable debe proporcionar al encargado los medios y las reglas para llevar a cabo la seudonimización.

11. ¿Se pueden conservar datos personales (como encargado) sin el consentimiento de mi institución (responsable del fichero)?

Respuesta: No.

Antecedentes: El artículo 24 del GDPR establece que «teniendo en cuenta la naturaleza, el alcance, el contexto y los propósitos de procesamiento, así como los riesgos de diversa probabilidad y severidad para los derechos y libertades de las personas físicas, el responsable del fichero implementará técnicas y medidas organizativas apropiadas para garantizar y poder demostrar que el procesamiento se realiza en conformidad con el presente Reglamento. Esas medidas serán revisadas y actualizadas cuando se considere necesario». Según el artículo 32, los datos personales no pueden procesarse sin instrucción expresa del responsable del fichero,

a menos que así se exija por decreto o ley. Además, el artículo 74 dictamina que debe establecerse la responsabilidad del responsable del fichero para cualquier procesamiento de datos personales realizado por el encargado o en nombre del responsable. El artículo 30 también versa sobre cómo responsable y encargado deben mantener registros de todas las actividades de procesamiento llevadas a cabo[1].

Recomendación: El encargado debería estar autorizado por el responsable de fichero (generalmente su institución sanitaria) para procesar datos visuales. El responsable es quien decide y gestiona los fines y medios del procesamiento de datos personales, de forma que se recomienda asegurarse de que su institución le permite mantener datos personales y es consciente de cómo los está procesando.

12. Si el personal sanitario (encargado) estuviera en posesión de datos personales, con el conocimiento de la institución sanitaria (responsable), ¿podría procesarlos de forma independiente?

Respuesta: No.

Antecedentes: Los artículos 24 y 74 establecen que el responsable es quien determina los propósitos y medios para el procesamiento de datos personales, mientras que el encargado cumple solo funciones de ejecutor. El encargado (en nuestro ejemplo, el personal sanitario) puede procesar datos únicamente bajo instrucción del responsable. Como ya se ha mencionado, el artículo 30 también establece como responsable y encargado deben mantener registros de todas las actividades de procesamiento. Según el artículo 32, los datos personales no pueden procesarse sin instrucción expresa del responsable, exceptuadas unas situaciones muy concretas (órdenes judiciales, etc.)[1,2].

Recomendación: Cada institución sanitaria tiene que informar claramente de quién es el responsable del tratamiento de los datos personales. La figura del responsable tiene que autorizar previamente cualquier procesamiento de datos que se quiera llevar a cabo.

13. ¿Se debe informar al paciente si sus datos de registros visuales se van a procesar para un propósito diferente a aquel para el cual dieron su consentimiento?

Respuesta: Sí, es siempre recomendable, aunque existen situaciones donde no hace falta.

Antecedentes: Se trata de uno de los principios fundamentales de la normativa GDPR. El «procesamiento posterior» de datos para fines más allá de aquellos para los que se obtuvo originalmente el consentimiento está sujeto a una serie de limitaciones de acuerdo con el GDPR. Se permite cuando el nuevo propósito es «compatible con los fines para los cuales se recopilaron inicialmente los datos personales». También para investigaciones científicas o fines estadísticos, y debe considerarse un procesamiento legal compatible. El responsable, después de haber cumplido con todos los requisitos para la legalidad del procesamiento original, debe tener en cuenta cualquier vínculo entre esos fines y aquellos del procesamiento posterior previsto, el contexto en el que se han recopilado los datos personales y, en particular, las expectativas razonables de los interesados, en función de su relación con el responsable en cuanto a su uso posterior. Además, también debería considerar la naturaleza de los datos personales, las consecuencias del procesamiento posterior previsto para los interesados y la seguridad apropiada para todas las actividades de procesamiento (originales y previstas)[1,2].

Recomendación: La situación más común a la cual se refiere este supuesto es la utilización de registros visuales para presentaciones en congresos, publicaciones científicas, etc. Si bien es verdad que la ley permite el «procesamiento posterior», esto es solo en casos muy concretos, como, por ejemplo, la investigación científica. En el caso de congresos o publicaciones científicas, es difícil argumentar que los registros visuales recogidos con fines clínicos se puedan utilizar (procesamiento adicional) sin consentimiento. Por esta razón, es recomendable incluir esta finalidad en los formularios de consentimiento informado, de manera que el paciente pueda ejercer sus derechos y que no se incurra en futuros problemas.

14. ¿Se pueden utilizar los registros visuales de un paciente fallecido?

Respuesta: Sí, pero con algunas precauciones.

Antecedentes: Las personas fallecidas no están incluidas en la normativa GDPR. Sin embargo, hay que asegurarse de que los datos personales de la persona fallecida no puedan considerarse como identificador indirecto de los residentes vivos de la UE[1].

Recomendación: Si las leyes institucionales o locales no lo prohíben, los datos personales de un paciente difunto pueden ser procesados sin consentimiento. Esto es muy útil en el caso de los registros visuales quirúrgicos, dado que la posibilidad de que haya identificadores indirectos de otros individuos es muy remota.

15. ¿Se pueden utilizar registros visuales que no cumplan con la normativa GDPR en un congreso en un país no perteneciente a la UE o para publicaciones fuera de la UE?

Respuesta: No.

Antecedentes: Según el artículo 3, el procesamiento de datos personales de un individuo que resida en la UE está sujeto a la normativa GDPR. La finalidad y el lugar donde estos sean utilizados carecen de importancia según el GDPR[1].

Recomendación: Cada vez que se procesen medios visuales que pertenezcan a residentes de la UE, hay que asegurarse del cumplimiento de la normativa GDPR.

16. Si se desea grabar registros visuales, ¿es necesario un formulario de consentimiento específico o se puede pedir permiso en el mismo consentimiento de otro procedimiento?

Respuesta: No se necesita un formulario de consentimiento por separado si el consentimiento para otro procedimiento se redacta de acuerdo con la normativa GDPR.

Antecedentes: El artículo 7 establece que «Si el consentimiento se otorga en el contexto de una declaración escrita que también implique otros asuntos, la solicitud de consentimiento se presentará de manera claramente distinguible de los otros asuntos, de forma inteligible y de fácil acceso, usando

un lenguaje claro y sencillo». Además, en caso de que el consentimiento incluya algún apartado no considerado legal según el GDPR, dicha parte pierde validez. Los pacientes deben ser conscientes de su derecho a revocar el consentimiento, pudiendo realizarse de forma sencilla[1].

Recomendación: Se recomienda la revisión de los formularios de consentimiento con el equipo legal de cada institución para que cumplan con los estándares de acuerdo con la normativa GDPR. Se aconseja declarar explícitamente que los registros visuales pueden ser anonimizados o seudoanonimizados y que pueden ser utilizados para fines educativos y científicos.

17. Si un paciente retira su consentimiento para el uso de registros visuales, ¿se pueden utilizar aquellos que ya tengamos en posesión?

Respuesta: Solo si se trata de datos anonimizados.

Antecedentes: El artículo 7 establece que «La retirada del consentimiento no afectará a la legalidad del procesamiento basado en el consentimiento antes de su retiro»[1].

Recomendación: Es recomendable anonimizar inmediatamente los registros visuales tras su grabación, ya que es la única forma de estar seguro de la legalidad de su uso en el futuro.

18. ¿Existe alguna manera de que el paciente renuncie a su derecho sobre sus registros visuales personales?

Respuesta: No.

Antecedentes: El cumplimiento del GDPR no es opcional y las personas (en este caso, el paciente) no pueden renunciar a sus derechos de protección de datos bajo la normativa GDPR[1].

Recomendación: No se le puede pedir a un paciente que renuncie a sus derechos de protección de datos de acuerdo con el GDPR. En la mayoría de los casos se pueden anonimizar legalmente los registros visuales.

19. ¿Hay alguna forma de utilizar registros visuales que no puedan ser anonimizados?

Respuesta: Sí, mediante la obtención de un consentimiento específico.

Antecedentes: La normativa GDPR permite el uso de datos personales con consentimiento explícito. Sin embargo, el interesado puede revocar el consentimiento en cualquier momento, lo que podría plantear problemas futuros (por ejemplo, para registros visuales ampliamente compartidos). Por esta razón, para los pocos casos que no puedan ser anonimizados, podría utilizarse un formulario de cesión de derechos de imagen (igual al que firman los modelos). De hecho, los fotógrafos utilizan contratos de cesión de derechos de imagen por escrito para el uso legítimo de los registros visuales obtenidos durante sus sesiones fotográficas[1,2,4].

Recomendación: En caso de tener que utilizar registros visuales que no puedan ser anonimizados, como la cara del paciente u otros identificadores directos (tatuajes únicos, cicatrices, etc.), el paciente debe firmar una autorización de cesión de derechos de imagen. Para estos casos inusuales, se recomienda encarecidamente consultar al equipo legal de su institución.

20. ¿Se pueden utilizar automáticamente registros visuales en un país de la UE si se cumple con el GDPR?

Respuesta: Sí, pero debe asegurarse de que no se infringen leyes institucionales o nacionales.

Antecedentes: Los Estados miembros de la UE tienen sus propias leyes y adaptaciones del GDPR según sus necesidades nacionales[1].

Recomendación: Cumplir con la legislación GDPR es la condición *sine qua non* para usar registros visuales legalmente. No obstante, se debe conocer la regulación interna de cada institución, así como las leyes nacionales, que pueden limitar el uso de registros visuales compatibles con el GDPR.

21. ¿Qué se debe hacer en caso de una filtración de datos que contenga datos personales?

Respuesta: Hay que informar al responsable tan pronto como se constate una posible filtración de datos.

Antecedentes: De conformidad con los artículos 33 y 34, el encargado notificará la sospecha al responsable tan pronto como sea posible. Si cabe la posibilidad de que exista un riesgo personal para el/los afectado/s, el responsable deberá notificar el evento sin demora a la autoridad nacional supervisora. La notificación debe hacerse en un periodo máximo de 72 h, y cualquier retraso debe ir acompañado de una razón válida. Si se considera poco probable que constituya un riesgo para el/los afectado/s, el responsable no tendrá que informar necesariamente de la fuga de información, pero deberá documentar tal decisión y justificarla. Si es probable que la filtración genere un alto riesgo para los derechos y libertades del/de los afectado/s, también debe informarle/s sin demora. Sin embargo, cabe enfatizar que si se decidiera que no es necesario notificar la filtración de información, debe poderse justificar tal decisión, por lo que esta debe quedar documentada[1].

Recomendación: Es recomendable ponerse en contacto con su responsable tan pronto como se objetive la filtración de información personal (acceso no autorizado a los datos, pérdida de datos, etc.), para que pueda realizar los trámites oportunos.

22. ¿Quién es responsable en caso de procesamiento ilegal de datos?

Respuesta: Tanto el responsable como el encargado pueden ser responsables en caso de procesamiento ilegal de datos.

Antecedentes: Según el artículo 32 y el considerando 146, la responsabilidad del procesamiento ilegal de los datos recae en último término sobre el responsable del tratamiento de los datos. El encargado solo es responsable si no ha cumplido con sus obligaciones de acuerdo con el GDPR o si hubiera actuado de forma externa o contraria a las instrucciones otorgadas por el responsable del tratamiento de los datos. Ni responsable ni encargado serán responsables si se demuestra que no han tenido nada que ver con el evento que da lugar al daño[1].

Recomendación: Se recomienda que los encargados (personal sanitario) no procesen nunca los datos personales de forma autónoma sin permiso del responsable. Al incumplir esta recomendación, al encargado se le podría otorgar responsabilidad directa y total.

23. ¿Quién es la persona responsable en caso de filtración de datos?

Respuesta: Los responsables de la filtración de datos personales serán el responsable y el encargado si no utilizaron el nivel de seguridad requerido para los datos que estaban procesando.

Antecedentes: De conformidad con los artículos 25, 32 y 82 y el considerando 83, tanto el responsable como el encargado deben garantizar un nivel adecuado de seguridad para la gestión de datos personales. Dependiendo de la clase de datos personales a manejar, podrían ser necesarios diferentes niveles de seguridad[1].

Recomendación: Es aconsejable que, en calidad de encargado, se asegure y exija que su responsable lleve a cabo una evaluación de posibles riesgos para decidir qué tipo de protección de datos debe implementarse.

24. ¿Cuáles son las sanciones por filtración de datos/ procesamiento ilegal de datos?

Respuesta: Las sanciones pueden ser muy graves, con multas de hasta 20 millones de euros.

Antecedentes: En virtud de los artículos 51, 83 y 84 y los considerandos 148, 149, 150 y 152, las autoridades supervisoras (autoridad pública independiente en cada Estado miembro, la Agencia Española de Protección de Datos) pueden imponer multas monetarias, mientras que los sistemas judiciales de los Estados miembros pueden imponer sanciones (penales y administrativas) de acuerdo con la legislación de cada Estado[1].

Recomendación: No hay que subestimar las sanciones y multas en las que se podría incurrir si no se cumple con la normativa GDPR.

Limitaciones

Como limitaciones en la metodología del artículo podría considerarse el hecho de que los autores hayan sido los mismos receptores del cuestionario realizado (proceso Delphi modificado *ad hoc*), sin añadir otros participantes. Por otro lado, el GDPR es muy complejo y difícil de interpretar y aplicar a la práctica médica, de forma que algunas recomendaciones no pueden ser claramente afirmativas o negativas.

En cuanto a la aplicabilidad internacional, este reglamento se encuentra vigente dentro de la UE, de forma que sería aplicable en los países que formen parte de esta. Sin embargo, hay que tener en cuenta que cada país puede tener su propia legislación particular, además de la expresada en el GDPR.

Conclusiones

El GDPR no resulta una lectura sencilla y sus tecnicismos son complejos y difíciles de comprender e interpretar. En esta guía se ha intentado dar una opinión objetiva sobre lo que el GDPR implica para los profesionales sanitarios cuando estos deciden utilizar datos personales y medios visuales, de una forma sencilla y comprensible para todos.

Los identificadores clínicos (datos personales, registros visuales, etc.) se encuentran diariamente en el ejercicio de la profesión médica y es importante conocer las implicaciones de compartirlos.

Se ha focalizado la discusión en los medios visuales dado que se trata de la información personal que se comparte más frecuentemente por parte del personal sanitario en varios ámbitos.

Actualmente sería imposible concebir la profesión médica sin el uso de registros visuales, ya que sin estos no se podría llevar a cabo la docencia como hoy la conocemos, o las presentaciones en cualquier congreso médico o publicación científica. Sin embargo, no hay que olvidar lo sensibles que son esos datos y las normas que rigen su uso.

Estas consideraciones son aplicables también a otros datos personales que estén bajo la regulación GDPR, aunque se necesitaría en algún caso un enfoque más específico.

A pesar de que la recopilación y difusión de datos personales pueda realizarse con buena voluntad y en el mejor interés del paciente, esto implica un riesgo para los profesionales sanitarios, cuyas connotaciones económicas no son nada desdeñables. Los autores esperamos que este trabajo estimule la creación de otras guías sobre otros aspectos de la gestión de datos en la profesión médica.

Conflicto de intereses

Luca Ponchietti, Alejandra Utrilla Fornals, Marta Roldon Golet, Melody García Domínguez, Alessandro Garcea y Peep Talving, declaran que no tienen ningún conflicto de intereses.

Nuno Filipe Muralha Antunes, declara el siguiente conflicto de intereses: es fundador y CEO de SurgeonMate, empresa de base tecnológica enfocada en mejorar el desempeño de la actividad quirúrgica.

BIBLIOGRAFÍA

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). OJ L 119, 4.5.2016, p. 1-88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV). [consultado 27 Ago 2020]. Disponible en: http://data.europa.eu/eli/reg/2016/679/oj
2. Spindler G, Schmechel P. Personal data and encryption in the European general data protection regulation. JIPITEC. 2016;7:163.
3. Ravikumar GK, Rabi BJ, Manjunath TN, Hegadi S R.S., Archana RA. Design of data masking architecture and analysis of data masking techniques for testing. Int J Eng Sci Technol. 2011;3:5150–9.
4. Teeples J. The business model. Morrisville, CA, Estados Unidos: lulu.com; 2016.