agencia española protección datos

Guía para profesionales del sector sanitario

Guía publicada en
junio 2022

ÍNDICE

PRESENTACIÓN

El Reglamento General de Protección de Datos de la Unión Europea incluye entre las funciones de las autoridades de Protección de Datos promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en esta materia; función que entre otros aspectos incluye la de facilitar mediante guías prácticas orientaciones que faciliten el cumplimiento de las mismas.

La Agencia Española de Protección de Datos (AEPD) ha sido particularmente proactiva en orden a facilitar información y orientaciones relativas al tratamiento de datos de salud dada la relevancia de los mismos al tener la condición de categorías especiales de datos y un régimen reforzado de protección. En este sentido, es necesario destacar la elaboración de la **Guía para pacientes y usuarios de la sanidad**, así como la creación en la página web de la AEPD de **un espacio dedicado específicamente a la información sanitaria**.

Con el fin de dar continuidad a estas iniciativas se ha planteado la elaboración de esta nueva Guía para profesionales de la salud, contribuyendo a facilitar el cumplimiento de esta normativa y la garantía de los derechos de los usuarios de sus servicios adaptada a las previsiones del Reglamento General de Protección de Datos (RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de carácter personal y garantía de los derechos digitales.

Sus principales destinatarios son los profesionales sanitarios que desempeñen su actividad a título individual, si bien sus orientaciones pueden resultar útiles en algunos aspectos para los profesionales que desarrollen su actividad en el marco de establecimientos sanitarios.

La guía comienza describiendo los conceptos básicos de datos de salud desde una perspectiva amplia para pasar a describir la posición jurídica de quienes intervienen en la prestación de servicios sanitarios como responsables del tratamiento de datos o como prestadores de servicios a dichos responsables (encargados del tratamiento en la denominación del RGPD).

A continuación, se describen las bases jurídicas para el tratamiento de los datos, diferenciando las que son específicas de los derechos de autonomía del paciente respecto de las del tratamiento de sus datos personales, que incluyen, junto con el consentimiento informado de los afectados, otras bases jurídicas que legitiman el tratamiento de sus datos personales sin necesidad de consentimiento.

El acceso a la historia clínica constituye un aspecto esencial de la asistencia sanitaria por lo que la guía facilita orientaciones sobre quiénes pueden acceder a la misma para las distintas finalidades para las que están legitimados, así como los riesgos y responsabilidades en que pueden incurrir quienes accedan ilícitamente.

En orden a facilitar el cumplimiento del principio de responsabilidad proactiva del Reglamento, también se facilitan orientaciones sobre las medidas a aplicar y sobre la garantía de los derechos de los afectados, con referencia específica a las limitaciones que pudieran tener en el marco de la normativa sanitaria.

Por otro lado, uno de los riesgos más habituales sobre la confidencialidad de los datos de los pacientes son las modalidades de acceso a su información cuando están internados en un centro sanitario o cuando son llamados para asistir a la consulta de los profesionales, por lo que la guía ofrece criterios específicos para minimizarlos. Adicionalmente se proponen soluciones para gestionar la seguridad de los recintos sanitarios y la identificación de los profesionales en los casos en que resulta procedente.

Por último, la guía trata de dar respuesta a las diversas situaciones que se plantean cuando los profesionales sanitarios desarrollan sus servicios en hospitales o clínicas, indicando los criterios que permiten identificar, en cada caso, quienes son los responsables del tratamiento de los datos de los pacientes y de las correspondientes historias clínicas.

1. CONCEPTOS BÁSICOS: DATOS DE SALUD, RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

A) ¿Qué tipo de datos trata un profesional sanitario y qué protección requieren?

Los profesionales sanitarios pueden tratar datos identificativos y de contacto de los pacientes (nombre, dirección, teléfono, DNI, etc.) y, principalmente, los relacionados con la salud, que sean necesarios para cumplir con la finalidad de prestarle la asistencia sanitaria relacionada con el servicio prestado. También pueden tratarse también datos identificativos de familiares como en el caso de menores, información relativa a los progenitores; o en el caso de personas con su capacidad limitada), referencia a datos de salud de estos como en el caso de enfermedades hereditarias u otros antecedentes familiares médicamente relevantes) y todos los datos útiles y necesarios para elaborar el diagnóstico y tratar al paciente.

Entre estos datos pueden señalarse, a modo de ejemplo, los datos relativos a costumbres alimentarias, al entorno geográfico, hábitos de los pacientes, viajes o la actividad física o deportes que practica.

Son datos de salud cualquier información que ofrezca una visión sobre su situación médica o estado de salud (presente, pasada o futura), incluida la prestación de servicios de atención sanitaria. Por ejemplo, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial o que permitan adquirir o ampliar conocimientos sobre su estado de salud física o mental, o la forma de preservarla, cuidarla, mejorarla o recuperarla (pruebas diagnósticas, medicación, etc.); el número o símbolo asignado a una persona a efectos de identificación sanitaria (número de Historia Clínica); la información procedente de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas; la información relativa a una enfermedad, a una discapacidad, al riesgo de padecer enfermedades, los datos facilitados por los familiares en los casos de menores o personas con capacidad cognitiva limitada, etc. Los datos de salud, además de la información facilitada por el paciente, pueden proceder de muy diversas fuentes (un profesional sanitario, un hospital o un dispositivo médico, entre otros).

Los datos de salud se encuentran dentro de las “categorías especiales de datos”, también conocidos como datos sensibles, por lo que merecen una protección reforzada y sólo se podrán tratar, es decir, almacenar, transmitir o revelar, entre otras formas de tratamiento, bajo ciertas condiciones y con determinadas garantías. Además, deberán adoptarse especiales medidas de privacidad, en particular de protección de datos desde el diseño y por defecto, seguridad y gestión de brechas de datos, así como los procedimientos oportunos y eficaces que garanticen un elevado nivel de protección, adecuado a los riesgos que existen en relación con los derechos de las personas.

B) ¿Quién es el responsable de los tratamientos de datos que se realizan?

El responsable es quien decide acerca de qué datos se van a obtener, con qué fines se van a tratar y con qué medios se van a gestionar y proteger. Puede ser tanto una entidad pública (hospital o centro de salud público) como privada (hospital/clínica), o un profesional a título individual.

El profesional sanitario será responsable del tratamiento cuando ofrece los servicios sanitarios a título individual o la entidad que lo contrata cuando trabaja por cuenta ajena. La entidad podría ser a su vez encargado de un responsable con relación a los tratamientos sanitarios cuando haya sido contratada para llevar a cabo los mismos de forma específica. En el caso que conjunto de profesionales trabajen en régimen cooperativo, podrán ser responsables respectivos del tratamiento que realice sobre los pacientes o,

en su caso, corresponsables de los tratamientos que formen parte de dicho régimen. El criterio relevante para determinar quién es responsable o corresponsable del tratamiento es el de identificar quién toma las decisiones sobre los fines y los medios del mismo.

C) Si contrato la prestación de ciertos servicios con un tercero, como la gestión de las Historias Clínicas ¿en qué condiciones puedo acceder a datos personales y de salud?

El tercero con el que se contrata la prestación de un servicio, que conlleva tratamiento de datos personales, se denomina encargado del tratamiento y el contratista tiene la obligación de ser diligente en seleccionar un encargado que ofrece las necesarias garantías de cumplimiento. La relación con el mismo debe realizarse mediante un contrato que ha de constar por escrito, incluso en formato electrónico, debiendo reunir su contenido unos requisitos. Así, es necesario identificar de forma clara y concreta cuáles son los datos y las instrucciones para el tratamiento de los mismos que realizará ese tercero y establecer la forma en que asegura el cumplimiento de las obligaciones de responsabilidad proactiva, como, por ejemplo, la correcta disponibilidad de un RAT, la existencia de políticas de protección de datos, la gestión del riesgo para los derechos y libertades, la aplicación de medidas de protección de datos desde el diseño y por defecto, la aplicación de medidas de seguridad orientadas a la protección de datos con relación a la confidencialidad, integridad, disponibilidad y resiliencia, la existencia de procedimientos para gestionar correctamente las brechas de datos personales, si ha nombrado un DPD, la adecuación a los requisitos de transferencias internacionales de datos, etc.

También deberá establecer que la entidad contratada asistirá al responsable en el cumplimiento de las respuestas a las solicitudes de ejercicio de derechos. Asimismo, se ha de prever el destino de los datos una vez finalizada la prestación, esto es, si se suprimirán o se devolverán los datos al responsable de la entidad contratante del servicio.

En todo caso, se ha de determinar la obligación del tercero de colaborar para demostrar que cumple con sus obligaciones en relación con la gestión de los datos personales y de salud, y permitirle al responsable la realización de auditorías o inspecciones en este campo.

Si el encargado del tratamiento subcontrata con otra entidad para la prestación de sus servicios tiene que informar sobre esta participación que debe ser autorizada por quién contrata los servicios del encargado.

La autorización puede darse de forma específica o general para los tratamientos que se refieran a una misma finalidad. Desde el punto de vista práctico es recomendable dar una autorización general para facilitar con flexibilidad la prestación de los servicios contratados (por ejemplo, almacenamiento, seguridad, software…).

2. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS

Como punto de partida, hay que tener en cuenta que el tratamiento de datos personales (incluidos los datos de salud) es toda operación que se puede realizar con los datos, como, por ejemplo, la recogida, su utilización para la prestación de un servicio, el acceso a los datos, su extracción, interconexión o la comunicación o cesión a terceros, la publicación de los datos, su conservación, modificación, alteración o supresión.

A) ¿Es necesario que el médico o el centro sanitario solicite el consentimiento a los pacientes para tratar sus datos personales? ¿O podría ampararse en otras bases legítimas?

En primer lugar, es necesario diferenciar entre el “consentimiento informado” para una actuación sanitaria (que se rige por la legislación sanitaria)

y el "consentimiento para el tratamiento de los datos personales", incluidos los de salud (al que es aplicable la normativa general de protección de datos). Nos centraremos solo en este último.

El tratamiento de los datos de los pacientes puede basarse tanto en dicho consentimiento como en otra causa prevista en una ley. Generalmente, no es necesario solicitar el consentimiento al paciente para tratar sus datos personales en el ámbito de la atención sanitaria. Así, por ejemplo:

- Cuando el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base de la legislación correspondiente o en virtud de un contrato con un profesional sanitario. Los datos deberán ser tratados por profesionales sujetos al secreto profesional o por alguien que esté bajo su responsabilidad.

  Aquí cabrían los tratamientos de datos que se realizan cuando se presta asistencia sanitaria por parte de centros o de profesionales sanitarios públicos o privados, incluida la asistencia prestada en el ámbito socio-sanitario. También se incluyen las actuaciones en materia de salud laboral (conforme a la normativa de prevención de riesgos laborales), con un acceso limitado por parte del empresario (aptitud o no del trabajador).

- Siempre que el tratamiento de los datos sea necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento. Por ejemplo, en caso de accidente o emergencia, cuando haya pérdida de consciencia del interesado.

- Cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o que los datos se requieran judicialmente. Por tanto, pueden tratarse datos de salud a propósito de un procedimiento judicial en el que dichos datos sean precisos (por ej., reclamaciones por negligencia médica, procesos de modificación de la capacidad, etc.), pero también para formular reclamaciones ante órganos administrativos u otros órganos no jurisdiccionales (arbitraje o mediación).

- Si el tratamiento de ciertos datos es necesario por razones de interés público en el ámbito de la salud pública, en los términos establecidos en la ley, como control de enfermedades transmisibles, epidemias, amenazas transfronterizas, etc.

- Cuando se realice con fines de investigación científica, de archivo en interés público o estadísticos, en los términos establecidos en la ley.

En los casos que se acaban de señalar pueden tratarse los datos de salud sin necesidad de consentimiento del interesado. Aunque sí será necesario informarle de determinados aspectos (por parte del médico, hospital público o privado, servicio de salud correspondiente, etc.); entre otros, de los siguientes: identidad y datos de contacto del responsable; datos de contacto del delegado de protección de datos, cuando éste exista; fines del tratamiento de los datos (asistencia sanitaria, investigación, etc.) y su base legítima (prestación de asistencia sanitaria, protección de intereses vitales, etc.); destinatarios a quienes serán entregados sus datos; plazo de conservación de los mismos; posibilidad de ejercitar los derechos reconocidos en la normativa de protección de datos o de presentar reclamación ante la agencia de protección de datos que corresponda. Y si, además, los datos no se han obtenido del propio interesado, es preciso informarle de las fuentes y las categorías de datos suyos que han sido recopilados hasta el momento.

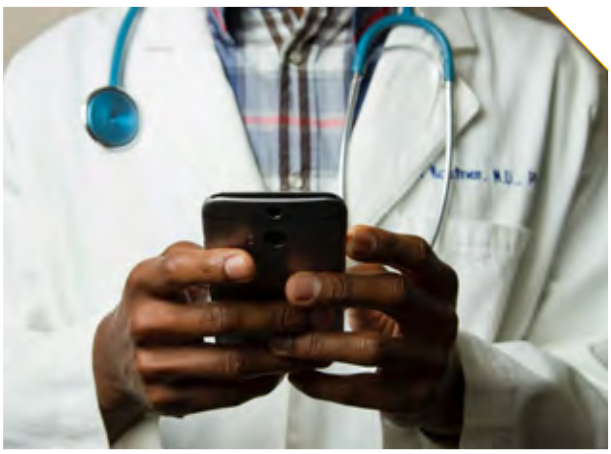
Hay muchos modos de informar al paciente de que sus datos están siendo recopilados: visualmente mediante señales o carteles, verbalmente en procesos de atención telefónica (la grabación de llamada facilitará la prueba) o por escrito (en

este caso también quedará constancia de que ha sido informado). Es fundamental en todo caso que la información sea veraz, de fácil lectura y comprensión (https://www.aepd.es/sites/default/files/2019-11/guia-modelo-clausula-informativa.pdf).

Respecto de la información que se facilita al paciente hay que tener en cuenta que la Ley de Autonomía del Paciente incluye un capítulo sobre el respeto a la autonomía del paciente que contiene toda una serie de informaciones, garantías y derechos que tiene el paciente desde la perspectiva sanitaria. Y, también, señala que, con carácter general, el tratamiento de la información del paciente desde esta perspectiva sanitaria se basa en su consentimiento.

Sin embargo, en lo que se refiere al tratamiento de los datos personales del paciente puede haber legitimaciones distintas de su consentimiento para el tratamiento de sus datos e informaciones específicas sobre los mismos. Por ello, con el fin de evitar confusiones respecto a la toma de decisiones sobre los derechos de autonomía del paciente y sobre el tratamiento de sus datos personales la información relacionada con estos últimos debería facilitarse de forma diferenciada y posterior a la que se haya facilitado respecto a la toma de decisiones sobre la autonomía del paciente.

Para otras actuaciones, como puede ser el envío de publicidad sobre otros servicios o el ofrecimiento de servicios no programados, por ejemplo, una clínica dental que contacta a un paciente después de haberle prestado el servicio para el que asistió a ese centro, con el fin de recomendarle que vuelva a dicho centro para hacerle una revisión o para cualquier otro tratamiento debe buscarse una legitimación específica como puede ser el consentimiento o también el interés legítimo del profesional sanitario o de la clínica siempre que se le haya informado sobre esta posibilidad, esté dentro de las expectativas razonables del paciente recibir la publicidad y garantizar que puede oponerse a su recepción en cualquier momento.



B) Si se trata de menores de edad ¿a partir de cuándo pueden prestar el consentimiento por ellos mismos para el tratamiento de sus datos (coordinación Ley 3/2018 y Ley 41/2002)?

El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

El consentimiento para las actuaciones sanitarias que lo exijan debe ser informado y por escrito. Ya se ha señalado, que para el tratamiento de datos personales con la finalidad de prestar asistencia sanitaria no es necesario solicitar el consentimiento del paciente, pero si es obligatorio informarle sobre el responsable del tratamiento, la posibilidad de ejercer sus derechos, las finalidades del tratamiento, (y todas las informaciones exigidas en el artículo 13 del Reglamento General de Protección de Datos). Si se facilitase esa información por escrito, es recomendable que vayan separadas la hoja del consentimiento sanitario dirigida al paciente de la hoja de información referida al tratamiento de sus datos personales.

C) ¿Pueden tratarse luego los datos con finalidades distintas a la asistencia sanitaria?

Si los datos se han recabado en el marco de la asistencia sanitaria y se han incorporado a una Historia Clínica (HC), su finalidad principal será la de facilitar dicha asistencia sanitaria.

No obstante, la ley permite en ciertos casos el tratamiento de datos incorporados a una HC con otros fines. Por ejemplo, con fines

judiciales, epidemiológicos, de salud pública, de investigación o de docencia, aunque la regla general en estos casos será la separación de los datos identificativos y los clínico-asistenciales (véase apartado de acceso a la HC).

El tratamiento posterior de los datos con fines de investigación científica (incluida la investigación en salud) podrá llevarse a cabo conforme en lo establecido en la normativa sectorial, basado en el análisis que propio responsable ha de realizar con relación a la compatibilidad de fines y en la aplicación de las necesarias medidas y garantías para la aplicación del principio de minimización. En particular, para la utilización de datos en materia de investigación en salud debe tenerse en cuenta lo previsto en la propia Ley Orgánica de Protección de Datos Personales (disposición adicional 17ª). (https://www.aepd.es/es/areas-de-actuacion/salud)

D) Tratamiento de los datos de los profesionales sanitarios: ¿Puede constar el nombre y apellido de los profesionales en las tarjetas identificativas? ¿Puede constar identificado un profesional sanitario en una reclamación hecha por un paciente para que intervenga como testigo?

Estaría justificado y sería proporcional que constara la identificación del profesional en una tarjeta identificativa claramente visible para el paciente, ya que puede ser necesario para éste conocer la identidad de la persona que le está prestando el servicio. Por ejemplo, para que el paciente pueda identificar al profesional que le ha atendido, y de este modo cerciorarse de que no ha habido confusiones.

Por otra parte, sí podría constar identificado un profesional sanitario a propósito de una reclamación hecha por un paciente, ya que existiría un interés legítimo en el tratamiento de estos datos o dicho tratamiento podría justificarse por el ejercicio del derecho a la tutela judicial mediante la presentación de una reclamación y también puede suceder que la identificación del profesional esta recogida como una obligación en la normativa aplicable en las distintas comunidades autónomas

3.¿QUIÉN Y CUÁNDO SE PUEDE ACCEDER A LA HISTORIA CLÍNICA (HC)?

En qué casos y condiciones se puede acceder por los médicos (¿pueden acceder también los residentes?); por inspección/evaluación/planificación (¿se puede acceder a la HC de pacientes para comprobar el proceso asistencial realizado por los profesionales que han tratado al paciente?); por personal administrativo; para docencia (¿puedo utilizar datos clínicos en cursos, clases, etc.? ¿pueden acceder los estudiantes en prácticas? ¿cabe acceso para la realización de TFG y TFM?); acceso por autoridades judiciales y administrativas (DGT, AEAT, otras administraciones competentes, mutuas de accidentes de trabajo y enfermedades profesionales…).

El acceso a la HC con el propósito de una atención eficaz y eficiente para la salud, especialmente en casos de emergencia vital, nunca puede limitarse con la excusa del cumplimiento de la normativa de protección de datos. Por otro lado, el responsable tiene la obligación de adoptar las políticas de control de acceso, de registro y trazabilidad de dichos accesos y de auditoría (automatizada y manual) de los registros para prevenir, detectar y corregir con diligencia cualquier abuso que se pueda producir.

El acceso a la historia clínica está limitado: no cualquier profesional y ante cualquier circunstancia puede acceder. Tanto el personal sanitario como otros profesionales pueden acceder a ella únicamente para el desempeño de sus funciones, sin que puedan revelar a terceros los datos a los que tienen acceso. Las posibilidades para acceder a los datos de la HC son distintas según el tipo de función profesional y de la finalidad del acceso a dichos datos:

ACCESO A LA HC POR PARTE DE PROFESIONALES SANITARIOS

¿A qué datos pueden acceder los profesionales sanitarios?

La finalidad de la historia clínica es fundamentalmente asistencial. Puede acceder a la historia clínica el profesional sanitario o el equipo directamente implicado en la asistencia al paciente o aquellos que sean consultados por éste con la finalidad de mejorar la atención terapéutica. En todo caso, el acceso estará limitado únicamente a los datos que sean precisos y, si no fuera necesario conocer la identidad del paciente, no se deberá acceder a la misma.

¿Pueden acceder a las HC los residentes?

El profesional residente puede acceder a los datos de la HC en los términos antes descritos, esto es, cuando sea necesario por razón de la atención sanitaria que está prestando. Los residentes tienen la consideración de profesional sanitario mientras dure su vinculación con el centro.

¿Puede accederse a la HC desde centros socio-sanitarios?

Los profesionales sanitarios en centros socio-sanitarios también deben poder acceder a las HC de los pacientes que están tratando, para poder prestar una correcta asistencia sanitaria.

¿Y desde centros privados concertados?

Los profesionales sanitarios de centros privados Los profesionales sanitarios de centros privados concertados deben poder acceder, si es necesario para prestar la atención sanitaria a un paciente derivado a ese centro, pero con acceso limitado a los datos necesarios para cumplir la función que le haya sido encomendada. Para ello deberán arbitrarse las medidas oportunas de manera que el centro de destino tenga conocimiento actualizado del estado de salud del paciente.

¿Podrá accederse por parte de los miembros de un Comité de Ética Asistencial?

Los miembros de estos Comités (algunos de los cuales pueden no ser profesionales sanitarios) accederán a la información que sea estrictamente precisa para emitir la correspondiente opinión ética que sea sometida a su consideración. Han de estar obligados por deber de secreto o firmar un acuerdo de confidencialidad. Solo cuando sea precisa la identificación para poder emitir el informe u opinión correspondiente, se accederá a ella.

¿Pueden acceder las empresas prestadoras de servicios a pacientes?

Las empresas proveedoras de servicios/equipos a los pacientes en domicilio tendrán acceso a los datos estrictamente necesarios para el cumplimiento de sus funciones. Como encargados del tratamiento, están obligados a cumplir con la normativa de protección de datos y solo utilizarán dichos datos siguiendo las instrucciones del responsable.

ACCESO POR PERSONAL ADMINISTRATIVO Y DE GESTIÓN

El personal de gestión y administrativo solo puede acceder a los datos de la HC necesarios para el ejercicio de sus funciones.

En esta situación se encuentra, en general, el personal de administración y servicios (servicio de admisión, personal encargado de atención al paciente, gestión de citas, gestión administrativa y de personal del centro, informática…), así como los cargos de dirección de un centro.

Todo el personal que acceda a los datos de una HC en el ejercicio de sus funciones está sujeto al deber de secreto.

ACCESO POR INSPECCIÓN/EVALUACIÓN/ ACREDITACIÓN

El personal con funciones de inspección, evaluación, acreditación y planificación tiene acceso a las HC en la medida necesaria para cumplir sus funciones (acreditación de la calidad de la asistencia, respeto a los derechos de los pacientes u otras obligaciones del centro en relación con los pacientes o la administración sanitaria).

Un inspector/a sanitario/a podría, por ejemplo, acceder a la HC de pacientes para comprobar el proceso asistencial realizado por los profesionales que los hubiesen tratado.

Este acceso está igualmente sujeto al deber de secreto.

ACCESO CON FINES DOCENTES

Los estudiantes cuando resulte necesario para su actividad docente o para la realización de prácticas, deberían tener un acceso limitado con un perfil de estudiante (como en cuanto al tiempo de acceso, funciones que puede desempeñar -modo consulta-, etc.). Solo deben acceder, con la oportuna autorización, a aquellos datos necesarios para su correcta formación y han de firmar el correspondiente compromiso de confidencialidad.

Para la realización de trabajos fin de grado y fin de máster la regla general debe ser el acceso a datos disociados (separados los datos identificativos de los datos clínicos).

El profesional sanitario puede utilizar los datos clínicos de pacientes con fines docentes (para impartir clases, cursos, etc.) siempre que no sea posible la identificación del paciente. Esto implica no sólo la separación entre datos identificativos y clínicos, sino también evitar su utilización en la medida de lo posible cuando, por las características del caso concreto, sea fácilmente identificable la persona de que se trata (por ejemplo, casos con trascendencia pública, casos raros que padezcan pocas personas y/o en lugares geográficamente pequeños, etc.). Esto mismo se aplicará cuando se quieran utilizar algunos datos en congresos, conferencias y similares. Para que se puedan utilizar datos en los que el paciente es identificable es necesario su consentimiento expreso.

ACCESO CON FINES DE SALUD PÚBLICA Y EPIDEMIOLÓGICOS

Los estudios epidemiológicos son necesarios para la prevención de los riesgos para la salud, así como la planificación y evaluación sanitaria y para ello requieren el tratamiento de datos de carácter personal y sobre la salud. El acceso a la HC con estos fines se debe llevar a cabo, separando los datos de identificación personal de los de carácter clínico asistencial, salvo que el paciente haya proporcionado el consentimiento para no separarlos.

Aun así, en este ámbito, podría accederse a los datos identificativos por razones de interés público, como cuando exista un riesgo o peligro grave para la salud de la población (por ejemplo, ante amenazas transfronterizas graves para la salud, control de epidemias, enfermedades transmisibles, etc.). Esto podría darse también para la incorporación de datos identificativos de pacientes en un registro de cáncer de una comunidad autónoma. En estos casos, deberán aplicarse garantías específicas, como que la persona que accede estará sujeta al secreto profesional y la Administración debe motivar la solicitud de acceso) y otros principios de protección de datos como la minimización de datos).

ACCESO CON FINES DE INVESTIGACIÓN

El acceso a la HC con fines de investigación científica, como regla general, se ha de hacer a datos disociados (separados los identificativos de los clínicos) y con las garantías adicionales que se establecen en la Ley de protección de datos personales (disposición adicional 17ª.2).

Podrán utilizarse datos de salud de personas identificadas para investigar, si se cuenta con su consentimiento. Este consentimiento puede ser amplio (puede solicitarse para áreas generales vinculadas a una determinada especialidad o servicio; así, en el ámbito del cáncer, ginecológico o de la reproducción...). También cuando el consentimiento se hubiera dado anteriormente para una determinada investigación y se quiera volver a utilizar los datos para una nueva investigación en un área relacionada con la anterior.

Estas reglas también serán aplicables a la investigación en salud pública y epidemiológica. Si bien las autoridades con competencia en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin necesidad de consentimiento de los interesados en situaciones de excepcional relevancia y gravedad para la salud pública.

Cuando sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere

la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.

El Reglamento Europeo de Protección de Datos y la nueva Ley Orgánica de Protección de Datos y garantía de los derechos digitales establecen criterios más flexibles que la legislación anterior para promover la investigación sanitaria. Puede obtener información más detallada a través del siguiente enlace (https://www.aepd.es/es/areas-de-actuacion/salud).

ACCESO CON FINES JUDICIALES

Cuando se solicite el acceso a una HC por parte de la autoridad judicial, se le proporcionarán a ésta los datos que solicite en el proceso correspondiente, pudiendo darse el acceso a datos no disociados cuando considere imprescindible la unificación de datos identificativos y clínico-asistenciales.

No obstante, sólo debe darse acceso a los datos imprescindibles para el caso de que se trate, evitando comunicar otros datos del propio sujeto o de terceros que no sean relevantes para el caso. A estos efectos, el órgano judicial debería tener en cuenta la necesidad o no de conocer datos que obren en la HC y que no tengan relación directa con el asunto a resolver. Así, por ejemplo, si se trata de un procedimiento de responsabilidad por una cirugía para reducción de estómago, ninguna relevancia tiene el hecho de que el mismo paciente se sometió a una intervención de vasectomía 12 años atrás; o que dicho paciente se sometió a una intervención de rinoplastia por una desviación del tabique nasal. En resumen, deberá ponderarse, por parte de la autoridad judicial, la pertinencia o, por el contrario, la inconveniencia, de acceder e incorporar en el expediente judicial la HC completa de una persona.

ACCESO POR AUTORIDADES ADMINISTRATIVAS

Al margen del acceso con fines epidemiológicos o de salud pública a los que se refiere la legislación sanitaria, las autoridades administrativas sólo pueden obtener datos de la HC cuando cuenten con el consentimiento del titular o así esté previsto en una norma legal de manera específica.

Así, por lo que se refiere a la Dirección General de Tráfico (DGT), ni la regulación general de protección de datos ni la de autonomía del paciente contemplan medida alguna al respecto, sin que tampoco se establezca en la normativa vigente en materia de circulación de vehículos a motor. En consecuencia, no se pueden ceder a las autoridades administrativas los datos personales relativos a la salud, salvo consentimiento de las personas afectadas.

En relación con las actuaciones de la Agencia Estatal de Administración Tributaria (AEAT), existe una obligación legal de proporcionar datos, informes, antecedentes y justificantes con trascendencia tributaria, es decir, relacionados con el cumplimiento de sus propias obligaciones tributarias o deducidos de sus relaciones económicas, profesionales o financieras con otras personas. Sin embargo, esta obligación no se extiende a los datos de salud, de manera que, en el caso de que se requiera el acceso a la HC, será necesario a eliminar la identificación de su titular.

4. LA RESPONSABILIDAD DEL PROFESIONAL SANITARIO

¿Puede derivarse responsabilidad y de qué tipo en el caso de acceso injustificado por el profesional sanitario a las HC?

Independientemente de las obligaciones del responsable, el personal sanitario que accede a una HC injustificadamente puede verse sujeto a distintos tipos de responsabilidad penal. disciplinaria y administrativa por protección

de datos, que en algunos casos pueden darse, incluso, de manera conjunta (por ejemplo, la indemnización a la víctima es concurrente con otras sanciones).

En primer lugar, este tipo de accesos está sancionado en el Código Penal como delito de descubrimiento y revelación de secretos. En dicho Código se prevén penas de hasta cinco años de prisión, según los casos, a las que se suman penas de multa, suspensión o inhabilitación. Por otro lado, cuando no tengan la suficiente gravedad para ser delito, estas conductas se podrán castigar con una sanción administrativa. En el caso de las entidades públicas, dicha sanción podrá consistir en el apercibimiento a la administración o entidad pública y, en su caso, se dará publicidad de la infracción cometida. Si se trata de centros privados, se aplicarán las correspondientes sanciones previstas en la normativa de protección de datos (entre ellas, la imposición de multas).

En el caso del profesional que realice su actividad en un centro sanitario, se le podrá imponer una sanción disciplinaria. Además, la vulneración del deber de confidencialidad que supone el acceso injustificado a la historia clínica es contemplada en la mayor parte de los Códigos deontológicos de las profesiones sanitarias como falta grave o muy grave, acarreando consecuencias que llegan hasta la inhabilitación profesional.

Por otro lado, el acceso indebido a la historia clínica puede dar lugar al deber de abonar a la víctima una indemnización de carácter civil, cuya cantidad dependerá de la valoración de los Tribunales.

Es importante recordar que la responsabilidad por el acceso indebido a los datos de la HC surge, no sólo por la revelación a terceros de los datos conocidos a propósito del acceso a la misma, que es lo que, en un primer momento, pudiera parecer más grave, sino que el profesional sanitario puede enfrentarse a todas o alguna de las consecuencias descritas simplemente con el mero acceso injustificado a la HC, incluidas las penas de prisión. Es decir, si se accede sin el consentimiento del paciente, o sin que concurra alguna de las finalidades protegidas por la ley (entre ellas, la más habitual, la prestación de asistencia sanitaria, que determina la consulta de los datos precisos para efectuarla), ese acceso ya es indebido y susceptible de conllevar consecuencias graves para el profesional. Sin perjuicio de que si, además, la información indebidamente consultada es revelada a terceros, las consecuencias legales serán todavía más graves.

En todo caso debe tenerse en cuenta que este tipo de conductas inciden también en las obligaciones relacionadas con la notificación de brechas de seguridad a las autoridades de protección de datos y, en su caso, la comunicación a los propios interesados. Y debe señalarse en el contexto de brechas de datos personales en el ámbito de la salud, la Agencia ha constatado que se están produciendo brechas de confidencialidad causadas por el acceso indebido de miembros de la organización a datos de la historia clínica de pacientes.

Otras brechas de datos personales similares notificadas con frecuencia en el ámbito sanitario son el envío de documentación con datos de salud o datos genéticos a destinatarios incorrectos, la destrucción sin garantías de confidencialidad de soportes de datos, o el extravío de muestras biológicas que permitan identificar al paciente.

Uno de los tipos de incidentes que están causando brechas de datos personales capaces de paralizar por completo la actividad de un profesional sanitario y que ocasionan un daño muy alto para los derechos y libertades de las personas son los ciberincidentes de tipo ransomware. El ransomware puede cifrar datos personales y sistemas informáticos, afectando a la disponibilidad de los datos y de los medios para tratarlos. En muchas ocasiones se produce también la exfiltración de los datos personales, lo que afecta a la confidencialidad. Estos incidentes suelen ir acompañados de intentos de extorsión tanto al profesional sanitario como a los pacientes afectados por la brecha, solicitando cantidades elevadas de dinero por recuperar y/o no hacerlos públicos.

La aplicación de medidas de seguridad preventivas específicamente destinadas a evitar este tipo de incidentes y disponer de sistemas de respaldo, no

solo de los datos, sino también de los servicios, es vital para minimizar el riesgo sobre las personas afectadas y dar cumplimiento a las obligaciones del Reglamento.

5. OBLIGACIONES EN EL TRATAMIENTO DE DATOS DE SALUD

A) ¿En qué medida el Reglamento General de Protección de Datos (RGPD) impone nuevas obligaciones?

Con carácter general, el profesional sigue teniendo las mismas obligaciones que con la anterior regulación: asegurarse de que el tratamiento de los datos sea lícito, informar al paciente de sus derechos y de que se va a proceder al tratamiento de sus datos y a respetar el deber de confidencialidad. Sin embargo, el RGPD impone nuevas obligaciones, precisa el alcance de otras y, sobre todo, exige que se pueda demostrar el cumplimiento de las mismas ("principio de responsabilidad proactiva").

En todo caso, con carácter general ha de tenerse en cuenta que:

- Es necesario realizar una gestión del riesgo que los tratamientos, tanto automatizados como no automatizados, de datos personales tienen en los derechos y libertades de los interesados. Para ello, se ha de tener en cuenta, entre otras circunstancias, la naturaleza, el alcance, el contexto y los fines en que se realiza el tratamiento de los datos.

- Con el fin de minimizar los riesgos, es necesario adoptar en los tratamientos y en su implementación las medidas y garantías que sean necesarias y proporcionales a dichos riesgos, en particular, implementar políticas de protección de datos, medidas organizativas, de protección de datos desde el diseño y por defecto, así como medidas de seguridad.

- Cuando las operaciones de tratamiento supongan un alto riesgo para los derechos y libertades, se ha de llevar a cabo una evaluación de impacto.

- Hay que disponer de un registro de actividades de tratamiento (RAT). En el caso de entidades públicas un inventario de tratamientos ha de ser publicado y estar accesible por medios electrónicos.

- Hay que nombrar a un Delegado de Protección de Datos (DPD), en los casos que sea obligatorio, con los conocimiento jurídicos, de gestión y técnico/científicos necesarios para informar, asesorar y supervisar al responsable en el cumplimiento de la normativa de protección de datos y salud de los tratamientos concretos que se lleven a cabo. El DPD ha de estar dotado con los recursos necesarios para ejecutar con eficacia sus funciones.

- El responsable ha de gestionar las brechas de datos personales para ser capaz de, al menos, notificar a la autoridad de control aquellas que constituyan un riesgo para los derechos y libertades y comunicar a los afectados aquellas que supongan alto riesgo. Estas acciones se han de realizar sin dilación indebida y, en el caso de las notificaciones, este plazo no puede superar las 72 horas. Además, han de documentar las brechas, sus efectos y las medidas adoptadas.

- En cumplimiento de la obligación de transparencia, la información al interesado sobre el tratamiento de sus datos deberá proporcionarse tanto en los casos en que los datos se obtengan directamente de la persona afectada como si, por el contrario, se hubiesen recibido por otras vías.

B) ¿Hay que nombrar un Delegado de Protección de Datos (DPD)?

La designación de un DPD es obligatoria cuando el tratamiento de los datos lo lleve a cabo una autoridad u organismo público y cuando se trate de centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de

los pacientes. Por tanto, los centros de salud y sanitarios públicos y privados han de disponer obligatoriamente de un DPD.

No obstante, quedan exonerados de la obligación de disponer de DPD los profesionales de la salud que ejerzan su actividad de manera privada a título individual, en cuyo caso no será necesario el nombramiento.

Su designación dependerá de la estructura y organización de los organismos de salud públicos y de los centros sanitarios privados. Se podrá designar a alguien de propio organismo o centro, o externo a los mismos. También podrá designarse un único DPD para varios responsables del tratamiento de datos, ya sean centros públicos o privados.

El DPD deberá cumplir los requisitos mencionados anteriormente, además de otras cualidades personales para ejercer sus funciones, como la de integridad y un alto grado de ética profesional.
Cuando se designe un único DPD para todos, o varios, centros sanitarios de un sistema de salud o de un grupo sanitario, es fundamental que esté fácilmente accesible desde cada centro para los interesados y la autoridad de control, así como también para los integrantes de los centros sanitarios.

Recomendaciones:

- Cuando se trate de profesionales sanitarios que ejercen su actividad a título individual, éstos podrían instar a sus respectivos colegios profesionales que le presten los servicios de DPD en el caso el que lo designen voluntariamente, para facilitarles el cumplimiento de la normativa de protección de datos.

Obligaciones

- Los responsables de los centros sanitarios, públicos y privados respaldarán al DPD en el desempeño de las funciones que tienen asignadas, facilitarán los recursos necesarios para su desempeño, el acceso a los datos personales y a las operaciones de tratamiento, y garantizarán que informen al más alto nivel de la organización y la formación necesaria para el mantenimiento de sus conocimientos especializados.

- Velar y adoptar las medidas adecuadas para que el DPD ejerza sus funciones en ausencia de conflictos de intereses y con total independencia.

- No despedir ni sancionar al DPD por el ejercicio de sus funciones.

C) ¿Cuándo tengo que hacer una evaluación de impacto?

La evaluación de impacto para la protección de datos (EIPD) es una obligación del responsable cuando, en el marco de la gestión del riesgo, se determine que el tratamiento suponga un alto riesgo para los derechos y libertades de los afectados. Para ayudar a determinar el nivel de riesgo de un tratamiento y, en su caso, la necesidad de realizar una EIPD, la AEPD ha dispuesto en su página web la herramienta EVALÚA_RIESGO.

Entre los factores de riesgo que hay que tener en cuenta están los derivados de la naturaleza del tratamiento, como sistemas de monitorización remota, telediagnóstico, toma de decisiones automatizadas , etc., el ámbito y la extensión, como abarcar gran parte de la población, colectivos vulnerables, datos genéticos, menores, etc., el contexto, como brechas en el entorno sanitario, sensibilidad social, etc., y los fines directos y colaterales, como perfilado, decisiones automatizadas sin intervención humanas, etc. Hay que tener en cuenta, que el tratamiento realizado por un profesional médico como consulta particular nunca se considerará a gran escala.

El DPD asesorará en la realización de la EIPD y supervisará su aplicación cuando hubiese sido nombrado. En caso de que no sea posible gestionar un alto riesgo, cabe la opción de presentar una Consulta Previa a la AEPD.

Para más información, puede consultarse la guía de Gestión del riesgo y EIPD, la Lista de verificación para determinar la adecuación formal de una EIPD y la presentación de consulta previa o los modelos

para la documentación de la EIPD para el sector público y privado.

D) ¿En qué casos hay que publicar el Registro de Actividades de Tratamiento (RAT) y de qué modo?

El responsable ha de mantener un registro en el que, al menos, conste la siguiente información de cada una de las actividades de tratamiento que lleve a cabo: la entidad responsable, la base legal para el tratamiento, los fines para los que se utilicen datos personales, el colectivo al que se refiera, la descripción de los datos que se manejen, si está prevista la comunicación a terceros o si van a ser transferidos internacionalmente, los plazos de conservación y, entre otros extremos, las medidas técnicas y organizativas de garantía de la seguridad y privacidad de los datos gestionados.

El RAT ha constar por escrito y, en su caso, en soporte electrónico, y estará a disposición de la Agencia de Protección de Datos o, si el responsable fuera una entidad pública, de la autoridad de control competente. Sin embargo, en el caso de las entidades públicas (incluyendo las fundaciones públicas) el inventario (art.31 LOPDGDD) con los tratamientos de datos personales deberá hacerse público y estar accesible por medios electrónicos (por ej., a través de la respectiva página web).

E) Medidas básicas de seguridad en el uso de dispositivos informáticos (control de accesos, gestión de claves, cambio contraseñas, envío de documentación clínica de forma cifrada; uso de tablets y otros dispositivos por parte de los profesionales, etc.).

Las medidas de seguridad son una de las medidas y garantías que ha de implementar el responsable para minimizar el riesgo para los derechos y libertades de los interesados. En función de la gestión del riesgo con relación a la protección de los datos personales, e integrada con otras obligaciones de seguridad del responsable, se ha de garantizar un nivel de seguridad, que incluya entre otros, la capacidad de garantizar la confidencialidad o de restaurar la disponibilidad y acceso a los datos en caso de incidente.

En particular, y debido a su impacto, el responsable, asesorado por su DPD, ha de ser consciente de qué brechas de datos personales se están produciendo en el contexto de sus tratamientos, para adecuar las medidas y garantías a adoptar.

Ejemplos de estas medidas a implantar en tratamientos de datos de salud serían:

- identificar los soportes utilizando sistemas de etiquetado comprensibles y con significado, que permitan a los usuarios con acceso autorizado identificar su contenido y dificulten la identificación al resto;
- codificar los datos en la distribución de soportes para que dicha información no sea accesible o manipulada durante su transporte;
- cifrar los contenidos de dispositivos portátiles cuando se encuentren fuera de las instalaciones, como memorias USB, y en la transmisión de datos a través de redes electrónicas (por ej. su envío por correo electrónico);
- conservar una copia de respaldo de los datos y de los procedimientos de su recuperación en un lugar diferente a aquel en que se encuentren los equipos informáticos que los tratan;
- guardar, como mínimo, de cada intento de acceso la identificación del usuario, fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado;
- cambiar las contraseñas que sirvan de mecanismo de autenticación como mínimo una vez al año y almacenarlas de forma confidencial. El uso de gestores de contraseñas facilita la posibilidad de recordar y mantener de forma segura contraseñas distintas y seguras en distintos servicios, así como cambiarlas periódicamente.
- Formación continua del personal.

A la vista de lo anterior, deben evitarse conductas tales como: facilitar el acceso a cualquier persona no apagando el ordenador, compartir claves y contraseñas, enviar información sanitaria mediante correos electrónicos o red pública abiertas, salvo que los datos se hayan cifrado o crear ficheros propios con datos personales de pacientes.

El empleo de medidas de seguridad, como otras medidas de gestión del riesgo para los derechos y libertades, no suple el incumplimiento en el tratamiento de los principios y derechos establecidos en el RGPD, en particular, la falta de una legitimación del tratamiento.

¿Es recomendable el uso de redes sociales y otros servicios similares para la gestión de citas o comunicaciones con los pacientes?

La gestión de citas o comunicaciones con los pacientes a través de redes sociales o de otros servicios como aplicaciones de mensajería instantánea, hay que tener en cuenta que tienen vinculado un tratamiento adicional por parte de un tercero. Por lo tanto, el responsable ha de ofrecer siempre medios alternativos de comunicación.

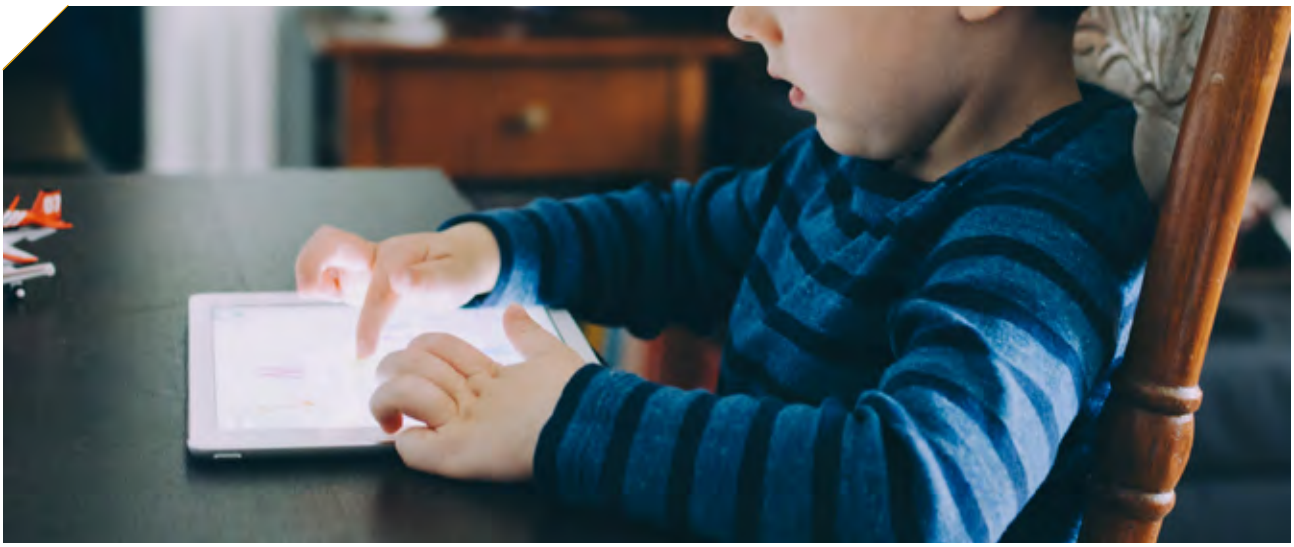
El tratamiento sería lícito si la finalidad del mismo es la prestación de la asistencia sanitaria o social y se refiere únicamente a datos personales que el interesado haya aportado o que se utilicen dentro de esa relación (por ejemplo, el número de teléfono). Por tanto, el responsable no podrá utilizar las redes sociales del paciente, pero sí su número de teléfono para notificarle o recordarle alguna cita u otra particularidad, siendo indiferente cuál sea la aplicación concreta utilizada, siempre que sea a través del teléfono (mediante una llamada o un mensaje de texto o instantáneo) y tal comunicación no llegue simultáneamente a personas no autorizadas (por ejemplo, si se utiliza una aplicación como Whatsapp u otras aplicaciones de mensajería similares, hay que asegurarse de que el mensaje se ha dirigido únicamente al paciente, y no a un grupo del que el paciente forma parte, aunque tengamos acceso al mencionado grupo).

Ahora bien, el tratamiento de datos de carácter personal que se hiciera a través de aplicaciones de mensajería instantánea está sujeto a los principios de protección de datos y el responsable tiene un grado de responsabilidad específico en la selección de los mismos, incluida la diligencia necesaria en la elección de los canales de comunicación más apropiados. En particular, en su empleo se ha de aplicar el principio de minimización de datos, revelando por estos cauces la mínima información necesaria. Además, ha de tenerse en cuenta que por la propia naturaleza de la relación clínica es posible que los contenidos de algunos mensajes transmitidos a través de esas aplicaciones contengan datos relativos a la salud, por lo que han de ser los propios responsables del tratamiento los que valoren la conveniencia de utilizarlas desde la perspectiva de la protección de datos, atendiendo por ejemplo a si disponen de un sistema de contraseñas débil o fuerte, siendo sencillo suplantar al usuario, o de si se cifran los mensajes o no. A la vista de las debilidades de unos u otros sistemas, por la ausencia de medidas de seguridad aceptables, es probable que no sea aconsejable la comunicación con el paciente a través de estos medios, especialmente cuando se trate de datos sensibles.

6. GESTIÓN DE LOS DERECHOS DE LOS PACIENTES RESPECTO AL TRATAMIENTO DE SUS DATOS

A) ¿Cuáles son estos derechos?

El Reglamento General de Protección de Datos regula como derechos de los afectados el de obtener confirmación del tratamiento de datos sobre si los mismos están siendo o no objeto del tratamiento y,en caso afirmativo, acceder a ellos. Asimismo regula los derechos de rectificación, supresión, oposición, limitación del tratamiento, portabilidad y a no ser objeto de



decisiones individuales automatizadas incluida la elaboración de perfiled.

Además, también se le debe notificar la destrucción, pérdida o alteración accidental o ilícita de sus datos personales, o la comunicación o acceso no autorizado, si esa violación supone un riesgo grave para sus derechos.

Sin embargo, en el ámbito sanitario, estos derechos se concretan en relación con la HC en la ley de autonomía del paciente y en la legislación autonómica sobre la materia, que se aplican como leyes especiales con carácter preferente al Reglamento Y, conforme a dicha normativa pueden ser objeto de algunas limitaciones (como la posibilidad de rectificar o suprimir datos de la HC); y otros tendrán escasa aplicación (como el derecho de oposición).

En general, estas limitaciones son consecuencia de la ley de autonomía del paciente, que obliga a conservar toda le información necesaria para conocer el estado de salud del paciente con el fin de garantizar la asistencia sanitaria. Lo que implica que dichos derechos puedan limitarse o modularse conforme a los criterios de los profesionales sanitarios que permitan garantizar la finalidad de ser necesarios para una adecuada asistencia sanitaria a los pacientes.

Y también porque la conservación de la historia clínica es necesaria para el cumplimiento de obligaciones legales, como es la de atender los requerimientos de los jueces, y por razones de interés público como la epidemiología o la evaluación de la calidad de la asistencia sanitaria, entre otras.

En todo caso la limitación de los derechos debe explicarse motivadamente a quienes los hayan ejercitado.

Para más información se recomienda consultar la guía para pacientes y usuarios de la Sanidad de la Agencia Española de Protección de Datos.

B) En el caso de menores de edad ¿Quién ejercita estos derechos? ¿Y si los progenitores están separados o divorciados?

A partir de los 14 años se le debe reconocer a un menor al menos el derecho a acceder a su HC, pues tiene derecho a estar informado de los asuntos que le conciernen. Esta información es básica para que pueda ejercer sus derechos a ser escuchado y a que su opinión sea tenida en cuenta en función de su edad y madurez.

Pero los padres y madres podrán acceder también a la historia clínica de sus hijos e hijas hasta la mayoría de edad, ya que son titulares de la patria potestad y tienen la obligación de velar por ellos y pueden intervenir en este ámbito para cumplir

con sus deberes de cuidado y asistencia. Esto no lo podrán hacer correctamente si no pueden conocer la información relativa a la salud de sus hijos.

Si los padres se encuentran separados o divorciados y ambos tienen el ejercicio de la patria potestad (aunque la guarda y custodia se le haya atribuido a uno solo de ellos), ambos deben estar informados y deciden sobre la salud de sus hijos y, en consecuencia, tienen acceso a su HC.

C) ¿A qué tiene derecho de acceso el paciente respecto de su HC? ¿Qué ocurre si se le entregan datos de un tercero?

Conforme a la normativa estatal sanitaria (Ley de Autonomía del Paciente), el paciente tiene derecho a acceder a la documentación de su propia HC y a los datos que constan en ella. En cambio, la normativa de protección de datos no reconoce el derecho de acceso a documentos concretos de la HC, sino a obtener confirmación de si se están tratando o no sus datos personales, y en caso afirmativo, derecho de acceso a los mismos mediante copia y a determinada información. En concreto, si los datos son obtenidos del interesado: identidad y datos de contacto del responsable, datos de contacto del Delegado de Protección de Datos, fines del tratamiento de los datos y base jurídica que sustenta dicho tratamiento, destinatarios o categorías de destinatarios y, en su caso, si van a realizarse transferencias internacionales de datos, el plazo de conservación de los datos personales o criterios para determinarlo, la posibilidad de ejercitar derechos; cuando el tratamiento se base en el consentimiento, la existencia del derecho a retirarlo, derecho a presentar reclamación ante autoridad de control, o la obligación de facilitar datos personales por ser requisito legal, y la existencia de decisiones automatizadas. Además, si los datos no han sido obtenidos del interesado, éste tiene derecho a conocer el origen de los mismos y las categorías de datos de que se trate.

No obstante, el derecho de acceso del paciente no incluye datos de terceras personas que consten en la HC en interés terapéutico del paciente, ni a las anotaciones subjetivas de los profesionales sanitarios, que se hayan opuesto a ello.

En el caso de que se entregaran datos de un tercero, se estaría vulnerando el deber de confidencialidad. En consecuencia, tanto la institución como el profesional podrían incurrir en responsabilidad, que puede ser administrativa (multa en el caso de institución privada o del profesional, apercibimiento en el caso e institución pública, disciplinaria para el profesional...), civil (si se ha causado un daño al tercero, éste podría tener derecho a una compensación a cargo de la institución y/o del profesional sanitario) y penal (multa o pena de prisión por revelar o ceder a terceros los datos de salud vulnerando la intimidad del paciente).

El paciente tiene derecho a conocer los accesos que se han producido a su HC (cuántos accesos, finalidad del acceso, etc). Pero, a día de hoy, ni la normativa sobre protección de datos, ni la normativa estatal sanitaria reconocen expresamente que este derecho incluya la identificación (nombre y apellidos) de los profesionales que han accedido a la historia clínica de un paciente (aunque podrían conocerse estos datos a propósito de una investigación judicial en curso por sospecha de acceso indebido). No obstante, algunas normas autonómicas sí reconocen la posibilidad de conocer la identidad de quién ha accedido, como Navarra y Extremadura, en cuyo caso el paciente podrá también solicitar estos datos cuando ejercite su derecho de acceso. En cualquier caso, la administración o centro sanitario tiene la obligación de implantar las medidas de seguridad necesarias para controlar y, en su caso impedir, el acceso por a la HC por parte de personas no autorizadas.

D) ¿En qué casos procede la rectificación de la HC si lo solicita el paciente?

El paciente tiene derecho a que se rectifiquen sus datos personales inexactos (mediante documentación acreditativa del error), por ejemplo, domicilio inexacto, apellido erróneo, etc.); y a que se completen sus datos personales incompletos, teniendo en cuenta los fines del tratamiento.

En el caso de rectificación de datos clínicos, será el facultativo que esté a cargo del paciente

quien determinará si procede dicha rectificación conforme a los criterios sanitarios aplicables

E) ¿Debe atenderse una solicitud de supresión de datos de la HC?

La supresión de datos de la HC está muy restringida, puesto que ésta tiene como finalidad principal garantizar una correcta atención sanitaria al paciente. Téngase en cuenta que las historias clínicas pueden cumplir también otras funciones secundarias de interés general (en salud pública, epidemiología, investigación, etc.). De ahí que el contenido de la HC no pueda quedar únicamente en manos del propio paciente. Es el profesional sanitario quien decide si procede o no suprimir un dato de la HC, en función de su trascendencia clínica.

Por ello, cuando se trate de datos sin relevancia para la asistencia sanitaria (Como datos relativos a cómo se produjo un accidente de tráfico que haya requerido asistencia médica y que no tengan trascendencia sanitaria), deberían poder suprimirse tales datos.

F) Si se ha eliminado incorrectamente documentación clínica ¿Cuál sería el tratamiento idóneo? ¿Hay que comunicarlo a la Agencia Española de Protección de Datos (AEPD) o, en su caso, a la Autoridad Autonómica competente?

Además de que se incumple la obligación de conservación de la historia clínica, en la medida en que esta documentación contenga datos personales nos podríamos encontrar en situaciones de brechas sobre la confidencialidad, disponibilidad o integridad de la HC, de donde se puede derivar la correspondiente responsabilidad legal (sanción, indemnización, etc,).

De forma no exhaustiva, algunos ejemplos de brechas de datos personales son:

- La destrucción accidental o pérdida de datos personales, total o parcial. Supone una brecha de disponibilidad y/o integridad si no existe otra copia recuperable de los datos.
- La destrucción incorrecta o incompleta de datos personales cuando debían ser eliminados, supone una brecha de confidencialidad dado que terceros no autorizados podrían acceder a esos datos.
- Ciberincidentes de tipo ransomware que provocan el cifrado de datos personales y sistemas de información impidiendo su tratamiento suponen una brecha de disponibilidad. Si, además, previamente al cifrado se ha producido exfiltración de los datos personales, supondrán también una brecha de confidencialidad.
- La alteración indebida o no autorizada de datos personales (por ejemplo, que un tercero altere o falsee el resultado de una prueba diagnóstica) supone una brecha de integridad.

En todos estos casos el profesional sanitario debe evaluar el riesgo que la brecha pueda suponer para las personas afectadas. Si existe tal riesgo, deberá notificarla a la AEPD, y también comunicarla a las personas afectadas si el riesgo es alto.

En la guía de la AEPD para la gestión y notificación de brechas de datos personales encontrará más detalles sobre cómo actuar en estos casos y cuándo y cómo deben notificarse y/o comunicarse estos incidentes.

7. GESTIÓN DE SITUACIONES QUE PUEDEN IMPLICAR COMUNICACIÓN DE DATOS A TERCEROS

A) ¿Cómo llamar a los pacientes en las consultas?

Toda persona tiene derecho a que se respete su intimidad en el ámbito de la salud, incluido el

carácter confidencial de los datos referentes a su salud. Por ello, para llamar a pacientes en las consultas deberá hacerse de manera que no se utilicen datos identificativos (como el nombre y apellidos, frente sino algún otro sistema proporcional a la difusión pública que se haga de los datos de salud (asignación de un código o número al paciente en el caso de utilizar monitores en los que se muestran pacientes de distintas consultas, utilización del nombre de pila al llamar por voz en un entorno que solo van a escucharlos los pacientes de la misma consulta, etc.).

B) ¿Cómo gestionar la información en mostradores de admisión para que no sea accesible al resto de pacientes que esperan?

Deben adoptarse medidas que permitan salvaguardar la intimidad del paciente y la confidencialidad de la información relativa a su salud. Por ejemplo, estableciendo la necesaria separación entre el paciente que está siendo atendido y el que espera; zonas separadas de admisión y salas de espera en la medida de lo posible, etc. El profesional encargado de la admisión deberá igualmente gestionar y comunicar la información de manera que no sea accesible a otros pacientes.

C) ¿Qué información debe prestarse para cancelar o posponer una cita por teléfono y cómo comprobar la identidad del interesado?

Para evitar la comunicación a terceros de datos de salud de una persona (sin su consentimiento) o la eliminación de dichos datos con el consiguiente perjuicio, deben establecerse mecanismos de identificación de la persona, para comprobar que se corresponde con el interesado (solicitando varios datos de identificación del paciente, nombre, DNI, número de tarjeta sanitaria, teléfono, etc., comprobando que coinciden con los que constan en la base de datos del centro). Adicionalmente, y partiendo de que es el interesado el que llama, preferentemente debería ser quien facilite la información sobre la cita que quiere posponer o cancelar.

Si es el centro el que llama, deberá hacerlo al teléfono o teléfonos facilitados por el propio paciente, informando en el momento inicial en que se recojan los datos de contacto de que se podrán utilizar esos números con tales finalidades.

En cualquier caso, deberá facilitarse la mínima información posible para identificar la cita (día, hora, centro, unidad), evitando hacer referencia a las posibles causas por las que se concertó dicha cita (por ejemplo, no mencionar síntomas, enfermedad, tratamientos, etc.).

D) ¿Qué información se puede dar cuando se llama a un hospital preguntando por un posible ingreso de una persona y/o la habitación en la que se encuentra y no se ha podido obtener el consentimiento del paciente?

No puede darse información sobre el ingreso de una persona y/o habitación en la que se encuentra si no se ha obtenido su consentimiento para facilitar dicha información. Si el paciente no se encuentra en condiciones de prestar el consentimiento (no está capacitado física o jurídicamente para hacerlo; por ejemplo, porque se encuentra inconsciente o es un menor de corta edad), podrán consentir los familiares. En cualquier caso, es importante que al paciente (o a los familiares) se les informe convenientemente sobre esta cuestión y sus consecuencias, antes de que presten el consentimiento.

No obstante, en situaciones excepcionales, tales como pacientes que ingresan en urgencias (cuyo consentimiento se recabará cuando sean trasladados a planta), pacientes inconscientes o personas desaparecidas, se podrá facilitar dicha información sin necesidad de consentimiento, pues la presencia de familiares o allegados puede ser esencial para la debida atención del paciente. En estos casos, únicamente se proporcionará información acerca de si la persona se encuentra en urgencias o ingresada y el número de habitación, sin indicar datos de salud o la atención médica prestada.

E) Gestión de los justificantes de asistencia de los acompañantes de pacientes ingresados ¿es necesario contar con el consentimiento del paciente? ¿debe comprobarse el parentesco?

No es necesario el consentimiento del paciente, puesto que el acompañante tiene un interés legítimo en obtener dicho justificante. Tendrá que justificar la vinculación/parentesco con el paciente.

En cualquier caso, la información que contenga el justificante debe ser la mínima imprescindible para la finalidad que tiene que cumplir (identificación del paciente, fecha/hora ingreso; duración del ingreso), sin que puedan incluirse datos que permitan identificar la causa que lo provocó (tipo de enfermedad, unidad de ingreso…).

8. GESTIÓN DE SEGURIDAD DE LOS RECINTOS

A) ¿Se pueden colocar cámaras de video vigilancia en los pasillos de consultas o salas de espera?

Sí, ya que la captación de imágenes por cámaras de videovigilancia en esos establecimientos abiertos al público está dirigida a aumentar y garantizar la seguridad tanto de las instalaciones como de los usuarios y pacientes.

Las cámaras sólo podrán captar esas zonas comunes, pero no estarán orientadas a las consultas, para evitar grabar su interior. Además, debe prestarse especial consideración a que han de instalarse, en los distintos accesos a esas zonas videovigiladas y, en lugar visible, uno o varios carteles informativos en los que se advierte de que se accede a una zona videovigilada. El cartel indicará de forma clara que se están tratando datos personales, la identidad del responsable, la posibilidad de ejercitar derechos y una referencia a dónde obtener más información.

En el caso de que dichas cámaras se quieran emplear con fines distintos a la seguridad, tales como control laboral, deberá informarse previamente a los profesionales y a los representantes sindicales.

B) ¿Es contrario a la normativa de protección de datos que el personal de seguridad de un centro sanitario solicite identificarse a personas que puedan resultar sospechosas?

No. El personal de seguridad tiene entre sus funciones efectuar controles de identidad para la protección del centro y de las personas que puedan encontrarse en el mismo, sin que en ningún caso pueda retener la documentación personal. La negativa a exhibir la identificación facultará al vigilante de seguridad a impedir a los usuarios el acceso al centro o a ordenarles su abandono.

9. LA POSICIÓN JURÍDICA DE LOS PROFESIONALES QUE PRESTAN SERVICIOS EN HOSPITALES O CLÍNICAS

Respecto de los criterios sobre la responsabilidad del tratamiento de datos de pacientes en los casos en los que el profesional sanitario es el que toma todas las decisiones sobre la atención a los mismos y al tratamiento de sus datos, aunque preste la asistencia sanitaria en un hospital, nos encontramos con tres supuestos:

El primer supuesto se refiere a un profesional sanitario que toma todas las decisiones sobre la atención sanitaria de sus pacientes, incluyendo el tratamiento de sus datos personales, prestando

sus servicios en un hospital o en una clínica, mediante el correspondiente arrendamiento de una consulta.

En este caso, donde la relación con el hospital o la clínica se limita al arrendamiento de un local, de un lugar, donde se presta la asistencia sanitaria, el profesional sanitario es el responsable del tratamiento de los datos personales de sus pacientes ya que es quien decide sobre los fines y medios del tratamiento. Así, en relación sobre la historia clínica de la que tiene la guarda y conservación de la misma, decide cómo suministra la información relativa a la protección de datos a sus pacientes, correspondiéndole la elaboración del RAT, la realización de la correspondiente EIPD y la implantación de las medidas de seguridad adecuadas, etc. O sea, se le atribuyen como responsable del tratamiento todas las obligaciones derivadas del RGPD en relación con el tratamiento efectuado.

Existe un segundo supuesto donde un profesional sanitario, si bien toma todas las decisiones sobre la atención sanitaria de los pacientes, se encuentra contratado para ello por el hospital o la clínica.

En este caso, donde los pacientes son del centro sanitario, el profesional sanitario es un empleado de la clínica u hospital. Por tanto, este último es, como responsable del tratamiento, quien tiene encomendadas todas las obligaciones en materia de protección de datos. Por ello, será el encargado de suministrar instrucciones a su empleado sobre cómo debe actuar en relación con la historia clínica, la cumplimentación de la misma, la determinación de las medidas de seguridad a seguir o qué hacer si solicitan los pacientes el ejercicio de uno de los derechos previstos en los artículos 15 a 22 del RGPD, entre otras cuestiones.

Un ejemplo de ello lo encontramos en el PS/00391/2020 dirigido contra IDCQ HOSPITALES Y SANIDAD, S.L.U. que finalmente se archivó.

Se reclamó por el profesional sanitario contra el centro de salud donde había prestado servicios, reclamándoles copia de la historia clínica de los pacientes que había atendido durante la vigencia de su contrato. Dado que el contrato no era laboral, sino mercantil, consideraba que *"la titularidad de los datos personales de las historias clínicas de los pacientes que he atendido en dicho centro hospitalario que incluye historias clínicas, no pueden mantenerse en el sistema informático del reclamado y deben ser custodiados y almacenados por el dado que el reclamado me considera empresario autónomo"*.

Sin embargo, tras una práctica de prueba muy minuciosa durante la instrucción del procedimiento, se constató que el reclamante no cumplía requisito alguno para poder ser considerado responsable del tratamiento, al no decidir ni sobre los fines ni sobre los medios del tratamiento.

https://www.aepd.es/es/documento/ps-00391-2020.pdf

En relación con el ejercicio de derechos, estos deben ser atendidos por el responsable del tratamiento. En el primero de los supuestos referenciados deberá atenderlos el profesional sanitario, mientras que en el segundo le corresponderá al centro sanitario.

Por último, en raras ocasiones nos encontramos con un tercer supuesto donde la relación jurídica entre el profesional sanitario y la clínica u hospital se desdibuja. En tales ocasiones acontece que el profesional sanitario atiende a sus propios pacientes en una consulta de la clínica u hospital, que compagina con la atención a los pacientes pertenecientes al centro sanitario, En estos casos habrá que determinar respecto de qué pacientes el personal sanitario o el centro de salud respectivamente son responsables del tratamiento o si comparten la determinación de los fines /o los medios del tratamiento, en cuyo caso nos encontraríamos ante un supuesto de corresponsabilidad.

Para dilucidar en todos estos supuestos quién es el responsable en cuanto al tratamiento de los datos personales, se ha de atender al caso concreto y al concepto funcional de responsable del tratamiento, tal y como deviene del Informe 0064/2020 del Gabinete Jurídico de la AEPD que, analizando las Directrices 07/2020 del Comité Europeo de Protección de Datos sobre los conceptos de responsable y encargado del tratamiento, afirma que el RGPD "*reitera que se trata de conceptos funcionales, que tienen por*

objeto asignar responsabilidades de acuerdo con los roles reales de las partes (apartado 12), lo que implica que en la mayoría de los supuestos deba atenderse a las circunstancias del caso concreto (case by case) atendiendo a sus actividades reales en lugar de la designación formal de un actor como "responsable" o "encargado" (por ejemplo, en un contrato), así como de conceptos autónomos, cuya interpretación debe realizarse al amparo de la normativa europea sobre protección de datos personales (apartado 13), y teniendo en cuenta (apartado 24) que la necesidad de una evaluación fáctica también significa que el papel de un responsable del tratamiento no se deriva de la naturaleza de una entidad que está procesando datos sino de sus actividades concretas en un contexto específico…".

No obstante, debemos matizar que en el ámbito público el responsable del tratamiento será siempre la autoridad sanitaria, pues es quien tiene encomendadas por la normativa las competencias sanitarias, lo que le exige determinar los fines y medios del tratamiento.

Y todo ello sin perjuicio de las obligaciones de secreto profesional que en todo caso tienen que mantener los profesionales sanitarios respecto de los datos de salud que conozcan en el ejercicio de su profesión.

En las consultas formuladas por los DPDs del ámbito sanitario en la reunión celebrada con ellos en 2019, se planteó una duda sobre la posición jurídica, como responsable o encargado del tratamiento de un laboratorio de pruebas diagnósticas.

El criterio de la Agencia fue que el laboratorio de análisis clínico que presta un servicio de asistencia sanitaria a través de pruebas funcionales o de laboratorio que ayudan al diagnóstico médico y prevención de la enfermedad, ha de ser considerado un centro sanitario, definido por el artículo 3 de la LAP como, "el conjunto organizado de profesionales, instalaciones y medios técnicos que realiza actividades y presta servicios para cuidar la salud de los pacientes y usuarios".

El artículo 14.2 de la LAP dispone que "Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información", añadiendo el artículo 17.1 de la propia Ley que "Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial".

Junto con el posible tratamiento que pudiera derivarse de la relación jurídica existente entre el laboratorio consultante y la entidad que solicita el servicio (ya se trate de otro centro sanitario o de una aseguradora), la LAP impone a aquél la obligación del tratamiento de los datos que hayan de incorporarse a la historia clínica del paciente, excediendo obviamente dicho tratamiento de "las instrucciones del responsable del tratamiento", lo que determina la imposible aplicación del artículo 28 del RGPD y la imposibilidad de considerar que el laboratorio como centro sanitario, sea un mero encargado del tratamiento de la entidad por cuyo encargo realiza los análisis clínicos.

Por este motivo, debe considerarse que el laboratorio consultante será responsable del tratamiento de datos personales de los pacientes, derivado de los análisis clínicos que haya efectuado.

www.aepd.es @aepd_es Linkedin AEPD