

TRATAMIENTO DE DATOS DE SALUD EN LA PRESTACIÓN DE SERVICIOS SOCIALES

Juan Luis Beltrán Aguirre

Doctor en Derecho

Asesor Jefe del Defensor del Pueblo de Navarra

SUMARIO: **I. DERECHOS FUNDAMENTALES AFECTADOS.** **II. MARCO NORMATIVO.** **III. LOS DATOS PERSONALES DE SALUD.** 1. Definiciones de datos de salud y de los documentos que pueden contenerlos. A. Datos personales relacionados con la salud. B. Historia Clínica. 2. Nivel de protección de los datos de salud: especial protección. **IV. EL TRATAMIENTO DE DATOS RELACIONADOS CON LA SALUD.** 1. Principios informantes de la recogida y tratamiento de datos de salud. 2. Obligaciones previas al tratamiento de los datos: creación, notificación e inscripción de ficheros de titularidad pública y privada. 3. La información y el consentimiento para el tratamiento de datos de salud. A. *La información debida.* B. *Excepciones al consentimiento expreso para el tratamiento.* 4. Medidas de seguridad en el tratamiento de datos de salud: aspectos generales. A. *Niveles de seguridad.* B. *Documento de seguridad.* C. *El responsable y el encargado del tratamiento.* D. *Prohibición de acceso sin autorización o habilitación legal y deber de secreto.* E. Prohibición de uso para finalidades incompatibles. 5. Medidas de seguridad de nivel alto aplicables a ficheros y tratamientos automatizados. 6. Medidas de seguridad de nivel alto aplicables a ficheros y tratamientos no automatizados. **V. EL ACCESO DEL PACIENTE Y USUARIO A SUS DATOS DE SALUD Y LA DISPONIBILIDAD SOBRE LOS MISMOS.** 1. Régimen jurídico del acceso. 2. Procedimientos o fórmulas de acceso. 3. Límites al acceso. 4. Derecho a la cancelación de los datos de salud. **VI. EL ACCESO A LOS DATOS DE SALUD POR PERSONAS DISTINTAS AL INTERESADO.** 1. El acceso por parte de familiares. 2. El acceso por parte de terceros o del público en general. 3. El acceso por facultativos sanitarios. 4. El acceso por personal de enfermería, trabajadores sociales, etc. 5. El acceso por profesionales sanitarios de centros, servicios y establecimientos concertados para la prestación de servicios. 6. El acceso a efectos de las actividades de inspección, evaluación, acreditación y planificación sanitaria. 7. El acceso a requerimiento Judicial, de la Fiscalía, del Defensor del Pueblo y de las Fuerzas y Cuerpos de Seguridad. 8. El acceso a efectos de responsabilidad patrimonial. 9. El acceso a efectos de funciones administrativas del centro, facturación de servicios sanitarios, etc. 10. El acceso a datos de personas fallecidas. 11. El acceso con fines históricos, estadísticos y científicos, así como epidemiológicos, de salud pública y de investigación. **VII. LOS DATOS DE SALUD DEL MENOR DE EDAD. PECULIARIDADES.**

I. DERECHOS FUNDAMENTALES AFECTADOS.

En el ámbito de la asistencia sanitaria son dos los derechos constitucionales afectados: el derecho fundamental a la intimidad personal regulado en el art. 18.1 CE, si bien el ámbito propio de este derecho es la intimidad corporal, y el derecho fundamental a la protección de datos derivado del art. 18.4 CE pues según doctrina del Tribunal Constitucional recogida principalmente en sus Sentencias 1993/254, de 20 de julio y 2000/292, de 30 de noviembre, contempla como un derecho fundamental independiente y desvinculado del derecho a la intimidad personal y familiar, aquel que tiene todo ciudadano a disponer libremente de sus datos.

Según señala la STC 2000/292, de 30 de noviembre, ambos derechos comparten el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar. Pero la peculiaridad del derecho fundamental a la protección de datos radica en su distinta función, objetivo y contenido. La función del derecho fundamental a la intimidad (artículo 18.1 CE) es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar. En cambio, el derecho fundamental a la protección de datos (artículo 18.4 CE) persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir un tráfico ilícito y lesivo para su dignidad. Así, el objeto del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino la reserva de todos los datos de carácter personal, particularmente los informatizados.

II. MARCO NORMATIVO.

El régimen jurídico de la protección de los datos de salud se articula a través de diversos instrumentos que operan en los ámbitos competenciales correspondientes: la Unión Europea, el Estado y las Comunidades Autónomas. En el ámbito europeo destacan las Directivas 95/46/CE y el art. 8 de

la Carta Europea de Derechos Fundamentales de 7 de diciembre de 2000. De la normativa nacional estatal cabe señalar, además de los citados artículos de la Constitución, la Ley 14/1986, General de Sanidad, la Ley Orgánica 15/1999, de Protección de Datos Personales, y su reglamento de desarrollo, la Ley 34/2002, de Servicios de la Información y Comercio Electrónico, la Ley 41/2002, básica reguladora de la Autonomía del Paciente, la Ley 16/2003, de Cohesión y Calidad del Sistema Nacional de Salud, la Ley 44/2003, de Ordenación de las Profesiones Sanitarias, la Ley 59/2003, de Firma Electrónica, la Ley 14/2006, de Técnicas de Reproducción Asistida Humana, la Ley Orgánica 7/2006, de Protección de la Salud y Lucha contra el Dopaje en el Deporte, la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, o la Ley 14/2007, de investigación Biomédica; todas ellas con su normativa de desarrollo, además de las normas de calidad aplicables, como la ISO 17799:2005. A este arsenal legislativo debe añadirse, además de otras normas estatales no citadas, la legislación autonómica existente, cuya sola cita excedería las posibilidades de esta presentación.

No obstante, las normas esenciales para el estudio que nos ocupa son las siguientes:

- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD).
- Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 de diciembre.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (LBAP), y Ley Foral 11/2002, de 6 de mayo, sobre los derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica.

Así pues, la problemática de la confidencialidad y protección de los datos de salud tiene que ser abordada desde dos ámbitos normativos distintos, que se complementan y que, por ende, han de integrarse para una aplicación conjunta y armónica: de un lado, desde la LOPD, que tienen el carácter de ley general para el tratamiento de datos personales, a la que ha de acompañarse su Reglamento de

2007, y, de otro, desde la LBAP y, en su caso, legislación autonómica, que es la ley especial en materia de protección y tratamiento de datos de salud.

III. LOS DATOS PERSONALES DE SALUD.

1. Definiciones de datos de salud y de los documentos que pueden contenerlos.

Tanto en la legislación de protección de datos como en la sanitaria encontramos diferentes referencias conceptuales para describir los datos personales de salud: historia clínica, datos de salud, datos genéticos, etc. Son conceptos diferentes, siendo el más amplio y genérico el de “datos relacionados con la salud”, y más específicos el de “historia clínica” o el de “datos genéticos”.

A. Datos personales relacionados con la salud.

Según el artículo 5. g) del Reglamento de la LOPD, los datos de carácter personal relacionados con la salud son “*las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética¹*”.

¹ Y. GÓMEZ SÁNCHEZ, en “*La protección de los datos genéticos: el derecho a la autodeterminación informativa.*” Revista D. y S., núm. extraordinario, 2008, p. 61, destaca la singularidad de la información genética obtenida mediante análisis de ADN de cualquier tipo y naturaleza resulta evidente. En general:

-Permite al propio sujeto obtener información sobre su configuración genética, las consecuencias presentes o futuras de tal configuración, y le posibilita la adopción de decisiones y el ejercicio de sus derechos y libertades.

- Permite identificar al sujeto, vivo o muerto, y/o relacionarle con otros sujetos vivos o muertos.

- Permite conocer al sujeto -pero también a terceros- el estado de salud actual y prever la mayor o menor propensión a padecer patologías futuras.

- Permite detectar predisposiciones genéticas de los individuos (no necesariamente de carácter patológico) y capacidades de diversa naturaleza.

- Aporta datos relevantes que pueden trascender el ámbito exclusivamente individual para afectar a la descendencia, a un grupo familiar o étnico determinado y, en última instancia, a un “patrimonio genético” común -pero diverso- de toda la Humanidad.

Por otra parte, el artículo 3 de la LBAP incorpora los conceptos de documentación clínica, entendida como “*el soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial*”; y de información clínica, referido a “*todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla*”.

Existen además otros conceptos que guardan una estrecha relación, tales como el de dato genético, definido en el art. 3.j) de la Ley 14/2007, de Investigación Biomédica, como la “*información sobre las características hereditarias de una persona, identificada o identificable obtenida por análisis de ácidos nucleicos u otros análisis científicos*”.

B. Historia Clínica.

Con carácter general el art. 3 de la LBAP, define la historia clínica como “*el conjunto de documentos que contiene los datos, valoraciones e informaciones de cualquier índole sobre la situación y evolución clínica de un paciente a lo largo del proceso asistencial*”. A su vez, artículo 15.1 artículo 15.1 completa la regulación de la historia clínica disponiendo que “*todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada*”. Por tanto, implícitamente establece el deber de elaborar la historia clínica de cada paciente.

Por su parte, el artículo 10.1 de la Ley Foral 11/2002 establece que la historia clínica recoge el conjunto de documentos relativos al proceso asistencial de cada enfermo, identificando a los médicos y demás profesionales asistenciales que han intervenido en el mismo. Añade que debe procu-

- Puede aportar información para el futuro aunque la relevancia de dicha información no se conozca en el momento de extraer las muestras biológicas;

- Aporta datos que podrían ser utilizados en campos muy diversos de la organización de las sociedades (cultura, medio ambiente, educación, biodiversidad...).

rarse la máxima integración posible de la documentación clínica de cada paciente, y que dicha integración debe hacerse, como mínimo, en el ámbito de cada centro, donde debe existir una historia clínica única para cada paciente

Su finalidad principal según el art. 15.2 de la LBAP es la de “...facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud”.

Así pues, la legalmente necesaria elaboración de la historia clínica persigue que se garantice al ciudadano la mejor asistencia sanitaria posible, lo que, además, debe conseguirse respetando los derechos fundamentales a la intimidad y a la protección de los datos. Por tanto, la historia clínica no tiene como norte la salvaguarda de los derechos fundamentales del artículo 18 CE y, a partir de ahí, garantizar la asistencia sanitaria, sino justamente lo contrario. Evidentemente, su elaboración y utilización exige la satisfacción íntegra de los tres derechos afectados, pero en caso de conflicto, no sólo de naturaleza jurídica, sino de otra índole, tales como organizativos, económicos o informáticos, cuando resulte forzado optar por la prevalencia de alguno de aquellos, entiendo que prima sobre los derechos fundamentales a la intimidad y a la protección de datos, el derecho a la asistencia sanitaria. Ello porque, en última instancia, así se preservaría el derecho fundamental a la vida, que es presupuesto del ejercicio del resto de derechos.

Las historias clínicas de los servicios públicos están informatizadas o en proceso de informatización. De ahí que convenga recordar que el Anexo de la Ley 11/2007, de Acceso Electrónico a Servicios Públicos, define el documento electrónico como “la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado”.

En el ámbito de los Servicios Sociales, la historia social es el equivalente a la historia clínica en los centros sanitarios.

2. Nivel de protección de los datos de salud: especial protección.

El artículo 7.1 de la LBAP establece que *toda persona tiene derecho a que se respete el carácter*

confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

Por su parte, el artículo 7 de la LOPD califica los datos de salud como especialmente protegidos y, al respecto, precisa en su apartado 3 que *los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.* Así pues, los datos de salud disfrutan de un estatuto jurídico particular dada su calificación de datos especialmente protegidos.

No obstante, añade el artículo 8 LOPD que las instituciones, los centros públicos y privados y los profesionales podrán proceder al tratamiento de los datos de salud de las personas que a ellos acudan o hayan de ser tratados en los mismos de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Y, en efecto, la legislación sanitaria, como veremos seguidamente, contiene normas específicas y prevé excepcionar el régimen de protección de los datos de salud del paciente, pudiéndose acceder a ellos, ser tratados o cedidos, cuando se pretenda evitar un daño a terceros, al propio paciente, o por imperativo legal.

IV. EL TRATAMIENTO DE DATOS RELACIONADOS CON LA SALUD.

1. Principios informantes de la recogida y tratamiento de datos de salud.

Me limito a enumerarlos pues ya han sido objeto de explicación por los ponentes que me han precedido.

- Proporcionalidad y exactitud.

- Limitación de objetivos, que en el ámbito sanitario no es otro que el de facilitar la asistencia sanitaria, si bien se contemplan algunas excepciones, como veremos.

- Exactitud de los datos.

- Cancelación de datos innecesarios, principio que, sin embargo, tiene importantes brechas en el ámbito sanitario, como también veremos.

- Transparencia y autonomía de la voluntad (lo que afecta a la información en la recogida de los datos, consentimiento en relación tanto con el tratamiento de los datos de salud como el acceso a los mismos, y el derecho de oposición al tratamiento).

- Confidencialidad y seguridad en el tratamiento.

2. Obligaciones previas al tratamiento de los datos: creación, notificación e inscripción de ficheros de titularidad pública y privada.

Fichero es todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Por tanto, manuales e informatizados.

Deben declararse todos aquellos ficheros que contengan datos de carácter personal, tanto si son informatizados, manuales estructurados o parcialmente informatizados (mixtos), siempre que estén identificadas o sean identificables las personas titulares de los datos.

No pueden crearse ficheros que contengan datos de carácter personal sin que se haya publicado la disposición que los crea. La LOPD tipifica como infracción grave “*proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente*”. También tipifica como infracción leve, cuando no sea constitutivo de infracción grave, “*no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos*”.

El contenido mínimo de la disposición de creación del fichero viene descrito en el artículo 54 del Reglamento LOPD².

² “La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.

b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter perso-

Actualmente, son muchos los centros de servicios sociales que también prestan una actividad sanitaria y socio-sanitaria. La actividad sanitaria se desarrolla por profesionales sanitarios. La asistencia social por trabajadores sociales. Entonces, se debe tener especial cuidado en diferenciar y separar el archivo y custodia de los datos de la historia social de aquellos que tienen como fin específicamente la asistencia sanitaria, que se integran en la historia clínica. La historia social sólo debe recoger aquellos datos de salud que repercutan en la situación personal y social del usuario de la prestación social.

En suma, es recomendable que se separen y se traten separadamente en distintos ficheros la historia social y la historia clínica, y que se configuren perfiles de acceso para cada profesional que trabaje en Servicios Sociales, de manera que sólo accedan a los datos necesarios para el ejercicio de sus funciones.

La complejidad que conlleva cada uno de los aspectos aludidos es enorme ya que se trata de un marco en el que el dato de salud merece una especial protección. Por ello, a los problemas generales que conlleva la aplicación de las medidas contempladas en la LOPD y su reglamento a cualquier fichero que contenga datos personales, se les añaden los particulares que se presentan cuando dichos datos personales son de salud.

Los ficheros de datos de titularidad privada deben ser notificados a la AEPD con carácter previo a su creación. La notificación debe incorporar

nal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.

c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.

e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.

f) Los órganos responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente Reglamento.”

similares datos a los públicos (artículo 55.2 del Reglamento de la LOPD).

La Agencia de Protección de Datos de la Comunidad de Madrid recomienda no autorizar la creación de Centros de Servicios Sociales hasta que hayan creado y registrado sus ficheros de datos de carácter personal.

3. La información y el consentimiento para el tratamiento de datos de salud.

A. La información debida.

En la primera fase del tratamiento de los datos, la autonomía personal se manifiesta en el derecho de los ciudadanos a conocer y determinar qué datos sobre su salud van a ser recogidos y registrados. Así, establece el artículo 5 LOPD que los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

En el ámbito de la información que nos ocupa es conveniente distinguir la información para el tratamiento de datos de salud de la información clínica para que el paciente pueda ejercer su derecho de autodeterminación a través del consentimiento informado. La primera se hace en los centros sanitarios normalmente a través de una leyenda en un impreso al entrar en el sistema sanitario, y en los centros y servicios de los Servicios Sociales se suele contener en los formularios de recogida de datos para la prestación correspondiente. La segunda como regla general se proporciona de forma

oral por el médico dejando después constancia en la historia clínica (artículo 4.1 LBAP).

En la información que se debe dar para la recogida de sus datos de salud, no tiene lógica ni sentido que cada vez que se hace un acto médico y se recaban nuevos datos, haya de practicarse nuevamente la información. Por el contrario, la información clínica ha de facilitarse cada vez que se hace un nuevo acto médico (artículo 4.2 LBAP).

Para dar cumplimiento al deber de información para el tratamiento de datos pueden utilizarse diferentes medios. Uno de los que propone la LOPD es la inclusión de textos informativos en los impresos y cuestionarios que se utilicen. De modo complementario pueden colocarse carteles informativos, accesibles a los ciudadanos, en los puntos en que se realice la recogida de los datos. En cualquier caso, para la recogida de los datos conviene analizar en cada supuesto concreto las peculiaridades del colectivo del que se están recogiendo (menores, mayores, discapacitados, etc.) y la forma más efectiva para que se dé cumplimiento al deber establecido legalmente. En cualquier caso, ha de llevarse a cabo a través de un medio que permita acreditar su cumplimiento (artículo 18 Reglamento LOPD) y corresponde al responsable del fichero la prueba del cumplimiento de la información.

Además de informar a la persona, también debe obtenerse su consentimiento expreso para tratar sus datos de salud o, en su caso, la existencia de una habilitación legal para ello³ (artículo 7.3 LOPD).

B. Excepciones al consentimiento expreso para el tratamiento de datos.

Las establece el artículo 6.2 en relación con el 7.6 LOPD en los siguientes términos: pueden ser objeto de tratamiento los datos de salud sin consentimiento cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asi-

³ Por ejemplo, Ley Orgánica de Protección de la Salud y de la Lucha contra el Dopaje en el Deporte; Ley sobre Tráfico y Circulación de Vehículos de Motor y Seguridad Vial; Ley de Prevención de Riesgos Laborales.

to profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto.

A lo dicho hay que añadir lo previsto en el artículo 8 LOPD en relación con los artículos 23 y siguientes de la Ley General de Sanidad, normas que habilitan a las instituciones y centros sanitarios, tanto públicos como privados, y a los profesionales, a proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratadas en los mismos de acuerdo con la legislación estatal o autonómica sobre sanidad. De este modo, basta con el consentimiento previo que se deriva de la relación de los usuarios con los centros y profesionales sanitarios para admitir también el tratamiento de sus datos sin necesidad de que presten un consentimiento específico. Al respecto, es preciso tener presente que tanto la LBAP como la Ley Foral 11/2002 parten del contrato verbal y obligan imperativamente a establecer un contenido mínimo de los datos sanitarios en las historias clínicas, contenidos mínimos que necesariamente han de ser tratados⁴.

⁴ El artículo 11 de la Ley Foral 11/2002, de 6 de mayo, establece el siguiente contenido de la historia clínica. 1. La historia clínica debe tener un número de identificación y debe incluir los siguientes datos: **a) Datos de identificación del enfermo y de la asistencia:** Nombre y apellidos del enfermo. Fecha de nacimiento. Sexo. Código de identificación personal contenido en la tarjeta sanitaria individual. Domicilio habitual y teléfono. Fecha de asistencia y de ingreso, si procede. Indicación de la procedencia, en caso de derivación desde otro centro asistencial. Servicio o unidad en que se presta la asistencia, si procede. Número de habitación y de cama, en caso de ingreso. Médico responsable del enfermo. **b) Datos clínico-asistenciales:** Antecedentes familiares y personales fisiológicos y patológicos. Descripción de la enfermedad o el problema de salud actual y motivos sucesivos de consulta. Procedimientos clínicos empleados y sus resultados, con los dictámenes correspondientes emitidos en caso de procedimientos o exámenes especializados, y también las hojas de interconsulta. Hojas de curso clínico, en caso de ingreso. Hojas de tratamiento médico. Hoja de consentimiento informado, si procede. Hoja de información facilitada al paciente en relación con el diagnóstico y el plan terapéutico prescrito, si procede. Informes de epícrisis o de alta, en su caso. Documento de alta voluntaria, en su caso. Informe de necropsia, si existe. En caso de intervención quirúrgica, debe incluirse la hoja operatoria y el informe de anestesia, y en caso de parto, los datos de registro. El informe de urgencia. La autorización de ingreso. El informe de anatomía patológica. En su caso, el documento de voluntades anticipadas, así como posible condición de donante de órganos. La evolución y planificación de los cuidados de enfermería. La aplicación terapéutica de en-

También pueden ser objeto de tratamiento los datos de salud cuando el mismo sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento. Subyace aquí la prevalencia del derecho a la vida sobre el derecho a la intimidad o la protección de datos personales (Según el TC sin vida no hay derecho a la intimidad: STC 1985/53).

4. Medidas de seguridad en el tratamiento de datos de salud: aspectos generales.

A. Niveles de seguridad.

Con carácter general los centros públicos de servicios sociales tendrán que implantar las medidas de seguridad adecuadas al grado de protección que requieran los datos contenidos en cada uno de los ficheros, atendiendo a lo dispuesto en las normas de aplicación.

Tanto para los ficheros automatizados como para los manuales (ubicados en archivadores, armarios u otros soportes) o parcialmente automatizados (mixtos), las medidas de seguridad se clasifican en tres niveles, básico, medio y alto, en función de la naturaleza de la información tratada.

Con carácter general, todos los ficheros manejados por los centros y servicios públicos que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico (sean automatizados, parcialmente automatizados –mixtos- o manuales). Además, todos aquellos ficheros que contengan datos de salud deben observar medidas de seguridad de nivel alto.

En el ámbito de los servicios sociales, con carácter general los ficheros deben tener medidas de seguridad de nivel medio o alto. No obstante, en lo que hace a concretos datos de salud precisa el artículo 81 del Reglamento LOPD lo siguiente:

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

fermería. El gráfico de constantes. El informe clínico de alta. **c) Datos sociales:** Informe social, si procede

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesorio se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

El alcance que la AEPD da a esta excepción en el informe jurídico emitido el 1 de julio de 2008, es el siguiente:

“En consecuencia, de lo señalado en el presente informe cabe concluir que será de aplicación la previsión contenida en el artículo 81.6 del Reglamento de desarrollo de la Ley Orgánica y, en consecuencia, será únicamente exigibles las medidas de seguridad de nivel básico en aquellos ficheros que contengan uno o varios de los siguientes datos:

- La mera indicación del grado de porcentaje de minusvalía del afectado o de los miembros de su unidad familiar a los efectos previstos para el cálculo de las retenciones en la legislación reguladora del Impuesto sobre la Renta de las Personas Físicas.
- La indicación de datos “apto” o “no apto” de un trabajador a los efectos previstos en la Ley de Prevención de Riesgos Laborales.
- Los datos relacionados con las obligaciones impuestas al empresario por la legislación vigente en materia de seguridad social que se limiten a señalar la existencia o no de enfermedad común, enfermedad profesional o accidente laboral o no laboral, así como la incapacidad laboral del trabajador.

Por el contrario, si el fichero contuviera cualesquiera datos relacionados con los resultados de las acciones de vigilancia de la salud distintos del meramente referido de aptitud del trabajador o incorporasen los datos relacionados con la concreta

enfermedad o accidente padecido por el trabajador, no será posible entender aplicable el artículo 81.6 del Reglamento, debiendo implantarse las medidas de seguridad de nivel alto.”

B. Documento de seguridad.

El responsable del fichero o tratamiento, tanto sea informatizado como manual, debe elaborar un documento de seguridad que recoja las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente, y que es de obligado cumplimiento para el personal con acceso a los sistemas de información.

El documento de seguridad puede ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También pueden elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, ha de tener el carácter de documento interno de la organización.

El documento debe contener, como mínimo, los aspectos reseñados en el artículo 88.3 del Reglamento de la LOPD.

C. El responsable y el encargado del tratamiento.

a) Centros públicos.

Conforme al artículo 3 de la LOPD el responsable del fichero es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

En los ficheros de titularidad pública, el responsable del fichero es el órgano administrativo que trata la información y tiene competencias en la materia, teniendo capacidad de decidir sobre el contenido, finalidad y uso del tratamiento de datos que se realiza. El responsable de un fichero debe indicarse expresamente en el correspondiente anexo de la disposición en la que se crea el mismo.

El Reglamento de desarrollo de la LOPD prevé la posibilidad de la existencia de varios responsa-

bles para un único fichero o tratamiento de datos de carácter personal (por ejemplo cuando en un centro sanitario se realicen diferentes actividades, siendo cada una de ellas competencia de diferentes órganos e instituciones sanitarias). En este caso, cada uno de los responsables debe notificar, a fin de proceder a su inscripción en el Registro de Ficheros de Datos Personales, la inscripción del correspondiente fichero.

Conforme al artículo 5 del Reglamento LOPD, el encargado del fichero es quien, en la práctica, trata físicamente los datos y los soportes, careciendo de autonomía y actuando siempre por cuenta y riesgo del responsable

En los hospitales, la gestión de un fichero de historias clínicas corresponde a las Unidades de Admisión y Documentación Clínica. Ahora bien, la custodia de dichas historias clínicas debe estar bajo la responsabilidad de la dirección el centro sanitario (artículo 17.4 LBAP). Por tanto, en los centros sanitarios corresponde la responsabilidad del fichero de historias clínicas a la dirección del centro.

b) Centros privados concertados.

No parece que una entidad privada que preste un servicio público en el marco de un contrato de gestión de servicios públicos, pueda ser considerado un simple encargado del tratamiento. Se trata de cesiones de datos en las que el centro contratado tiene el carácter de responsable del fichero, que es privado, al llevar a cabo una actividad asistencial y conservar con esa finalidad la historia clínica⁵. Recuérdese que la LBAP atribuye la responsabilidad del fichero a cada centro sanitario y al profesional individual, que deben conservar las historias clínicas de sus pacientes. El paso de un modelo de historia clínica descentralizada en cada uno de los centros a un modelo de historia clínica centralizada e informatizada a nivel de Servicio Autonómico de Salud transforma estas cesiones de historias clínicas en accesos dentro del marco del mismo responsable del fichero.

De todo lo anterior, puede inferirse que en el ámbito de los Servicios Sociales, el responsable

del fichero es cada Centro o Servicio, ello sin perjuicio de que la gestión y custodia del fichero pueda encomendarse a una concreta unidad.

D. Prohibición de acceso sin autorización o habilitación legal y deber de secreto.

a) Prohibición de acceso.

Recordemos que el artículo 7.1 de la LBAP establece que nadie puede acceder a datos de salud sin previa autorización amparada por la Ley.

El artículo 197.2 del Código Penal tipifica como delito el que, sin estar autorizado, acceda a datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

b) Deber de secreto.

El derecho a que se mantenga la confidencialidad de los datos de salud tiene como reverso el deber de secreto de quien accede a los mismos para el desempeño de sus funciones. A partir de la LBAP se ha producido una ampliación de los sujetos tradicionalmente obligados al secreto profesional, en cuanto su artículo 16.6 hace recaer esta obligación sobre cualquier persona que tenga acceso a la información contenida en las historias clínicas.

Por su parte, el artículo 10 LOPD establece que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsisten aún después de finalizar sus relaciones con el titular del fichero, o, en su caso, con el responsable del mismo.

El art. 199.2 del Código Penal tipifica como delito la revelación de secretos profesionales. Según expresa la STS de 4 de abril de 2001 para el ámbito sanitario “*Se trata de un delito especial propio, con el elemento especial de autoría derivado de la exigencia de que el autor sea profesional, esto es que realice una actividad con carácter público y jurídicamente reglamentada. La acción consiste en divulgar secretos de otra persona con incumplimiento de su obligación de sigilo, tal obligación viene impuesta por el ordenamiento,*

⁵ En este mismo sentido se pronuncia el informe 0501/2005 de la Agencia Española de Protección de Datos.

Ley General de Sanidad 14/1986, de 25 de abril, cuyo artículo 10.3 establece el derecho de los ciudadanos tienen derecho «a la confidencialidad de toda la información relacionado con su proceso y con su estancia en instituciones sanitarias» y concurrente en el historial clínico-sanitario, en el que deben «quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica» (art. 6.1).»

Por su parte, el artículo 44 de la LOPD tipifica como infracción administrativa leve, grave o muy grave, el incumplimiento del deber de secreto profesional.

E. Prohibición de uso para finalidades incompatibles.

Establece el artículo 4.2 LOPD que *los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.*

La Sentencia de la Audiencia Nacional, de 12 de junio de 2007 –JUR 199159–, elabora el siguiente concepto de “fines incompatibles”:

Respecto de la interpretación del término finalidades incompatibles, la SAN, Sec1ª, de 17-3-2004 (rec.641/2001) señala "Cuando el art. 4.2 de la LOPD, CE del Parlamento y del Consejo, de 24 de octubre de 1995, pero la trasposición del término incompatibles resulta confusa y equívoca y como tal ha quedado plasmado en el derecho español. Baste señalar que un dato de carácter personal recabado para una determinada finalidad puede ser indebidamente utilizado para otra actividad diferente que sin embargo no sea estrictamente incompatible con aquella. Aplicando de forma literalista el artículo 4.2 de la Ley Orgánica, quedaría privado de sentido y vaciado de contenido y para evitar este resultado indeseable esta Sala considera que lo que prohíbe el precepto es que los datos de carácter personal se utilicen para una finalidad distinta de aquella para la que han sido recogidos".

En este sentido la SAN 11-2-2004, que a su vez sigue el criterio de la de 8-2-2002, dice

«En relación con la interpretación de la expresión finalidades incompatibles que establece el art. 4.2 de la Ley Orgánica 15/1999, esta Sala no puede compartir el criterio que postula el recurrente, pues aunque el artículo 4.2 de la Ley 5/1992, ya no se refiere a "finalidades distintas", sino a "finalidades incompatibles", revelando una ampliación de la posibilidad de utilización de los datos, sin embargo la interpretación sistemática del precepto y la ambigüedad del término finalidades incompatibles avalan la interpretación realizada en el acto administrativo impugnado. En efecto, según el diccionario de la Real Academia "incompatibilidad" significa "repugnancia que tiene una cosa para unirse con otra, o de dos o más personas entre si", por tanto una interpretación literal ampararía el uso de los datos para cualquier fin abriendo una gama indefinida e ilimitada de finalidades, pues es muy difícil imaginar usos que produzcan la repugnancia que evoca la incompatibilidad, por lo que "semejante interpretación conduce al absurdo y como tal ha de rechazarse. Teniendo en cuenta, además, que dicho término se introduce en la Ley de 1999, como ha declarado la doctrina, por una traducción poco precisa del artículo 6 de la Directiva 46/1995, de 24 de octubre." Conclusión igualmente avalada por la interpretación sistemática aludida, pues como señalábamos en la citada sentencia de febrero de 2002, "semejante prescripción no puede ser entendida sino como un enunciado de carácter general, que no puede prevalecer sobre la regulación específica de una materia" citando al efecto el artículo 6 de la citada Ley, y añadiendo que la interpretación de dicho art. 6.2, a sensu contrario, impone "que cuando los datos se usen con otra finalidad distinta se precisará el consentimiento del afectado". Y no parece que el art. 4.2, venga a efectuar una ampliación sobre la posibilidad de utilización de los datos, porque ello supondría dejar sin contenido el art. 6.2, cuya redacción en este punto es igual a su homónimo de la Ley 5/92».

En conclusión, si la recogida o entrega de datos de carácter personal se realizó con unos fines determinados, cualquier uso o tratamiento posterior que no esté en consonancia con las finalidades para las que fueron facilitados y sobre las que el afectado no consintió, es in-

compatible con la finalidad que determinó la entrega, utilizando la LOPD la expresión finalidades incompatibles como sinónimo de finalidades distintas.

5. Medidas de seguridad de nivel alto aplicables a ficheros y tratamientos automatizados.

El documento electrónico, normalmente historia clínica electrónica, se ha de gestionar mediante el sistema o soporte de información específicamente creado al efecto, con la finalidad de garantizar la calidad, accesibilidad y seguridad técnica de la información clínica, así como la coordinación y la continuidad asistencial.

Los profesionales que necesiten cumplimentar o consultar la historia clínica electrónica de un paciente o usuario deben utilizar exclusivamente el sistema o soporte creado.

Los datos de salud, como datos especialmente protegidos, han de tratarse y cederse en los términos previstos en los artículos 7, 8 y 11 de la LOPD y 101 a 104 del Reglamento de la LOPD.

De entrada, no es necesario el consentimiento de la persona interesada para la comunicación de datos de salud a través de medios electrónicos, entre organismos, centros, servicios y establecimientos del Departamento de Salud y del Departamento de Asuntos Sociales, así como entre estos.

El sistema o soporte que se implante debe identificar de forma inequívoca y personalizada a todo profesional que intente acceder a la información contenida en la historia clínica de un paciente o usuario, y ha de verificar su autorización.

Deben establecerse las medidas técnicas y operativas de control de los accesos de los profesionales a la información contenida en la historia clínica. Normalmente este acceso se realiza mediante el uso de la tarjeta identificativa del profesional y su firma electrónica reconocida.

De cada intento de acceso al sistema se debe guardar, como mínimo, la identificación del profesional de que se trate, la fecha y hora en que se realizó, la parte de la historia clínica accedida y el tipo de acceso. Si el acceso al sistema es denegado por no cumplirse los criterios de acceso, esta denegación debe quedar también registrada.

En el Servicio Navarro de Salud-Osasunbidea la historia clínica está informatizada. Hablamos, entonces, de historia clínica electrónica. Ésta permite establecer distintos mecanismos de seguridad a efectos de la protección de los datos, imposibles de realizar con historiales tradicionales en formato papel.

6. Medidas de seguridad de nivel alto aplicables a ficheros y tratamientos no automatizados.

Una de las grandes novedades introducidas por el Reglamento de la LOPD es la regulación de las medidas de seguridad de los ficheros no informatizados. La hace en los siguientes términos:

A. Almacenamiento de la información.

- Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deben encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deben permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

- Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable debe adoptar medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

B. Copia o reproducción

- La generación de copias o la reproducción de los documentos únicamente puede ser realizada bajo el control del personal autorizado en el documento de seguridad.

- Debe procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

C. Acceso a la documentación.

- El acceso a la documentación se ha de limitar exclusivamente al personal autorizado.

- Se deben establecer mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

- El acceso de personas no incluidas en el apartado anterior debe quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

D. Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deben adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

V. EL ACCESO DEL PACIENTE Y USUARIO A SUS DATOS DE SALUD Y LA DISPONIBILIDAD SOBRE LOS MISMOS.

1. Régimen jurídico del acceso.

El artículo 18.1 LBAP establece que el paciente tiene derecho de acceso, con las reservas que comentaré, a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Además, en la normativa autonómica nos encontramos con especificaciones que suponen un avance sustancial al respecto. Así, el artículo 5.1 de la Ley Foral 11/2002, sobre los Derechos del Paciente a las Voluntades Anticipadas, a la Información y a la Documentación Clínica, añade el derecho “*a conocer en todo caso quién ha accedido a sus datos sanitarios, el motivo del acceso y el uso que se ha hecho de ellos, salvo en caso de uso codificado de los mismos*”.

El derecho de acceso a los datos de salud se ostenta a partir de los 14 años de edad. Así lo entiende la AEPD, criterio que comparto.

2. Procedimientos o fórmulas de acceso.

El citado artículo 18.1 también obliga a los centros sanitarios a regular el procedimiento que garantice la observancia del derecho de acceso. Por su parte, el artículo 14.1 de la Ley Foral 11/2002 establece que corresponde a la Administración regular el procedimiento que garantice el acceso.

Hasta el momento, la Administración de la Comunidad Foral no ha regulado dicho procedimiento.

En todo caso, conforme a los artículos 23 a 30 del Reglamento de la LOPD el acceso se hará a través de las siguientes formas:

- El acceso ha de ser ejercitado por el interesado, acreditando su identidad, o por representación voluntaria o legal (incapaces, incapacitados).

- El acceso a la historia clínica debe articularse de forma sencilla y a través de un procedimiento gratuito sin que, en ningún caso, pueda suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan (artículo 23.4). No parece, por tanto, que puedan establecerse tasas o precios públicos por la obtención de copias de las historias clínicas.

- Debe concederse al afectado su derecho de acceso ante los servicios de atención al paciente de los centros sanitarios (art. 24.4). Entiendo que lo mismo en los de servicios sociales.

- Las solicitudes de acceso deben contener las menciones mínimas exigidas por el art. 25 del Reglamento de la LOPD⁶.

- Las solicitudes de acceso deben ser resueltas en el plazo máximo de un mes a contar desde la fecha de su recepción, y hacerse efectivas en la propia respuesta o en el plazo de los diez días siguientes (art. 29). El interesado puede optar por recibir la información mediante visualización en pantalla, escrito, copia o fotocopia remitida por correo certificado o no, correo electrónico o cual-

⁶ a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición en que se concreta la solicitud.

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

quier otro sistema adecuado a la configuración o implantación material del fichero (art. 28).

- El derecho de acceso incluye conocer la identidad de los profesionales que han incorporado datos a la historia clínica, incluso las cesiones realizadas o previstas.

- El derecho de acceso sólo puede ser ejercido en intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo, en cuyo caso podrá ejercerlo antes. El problema es que resultará complejo determinar cuando hay un interés legítimo y cuando no.

3. Límites al acceso.

El derecho de acceso del paciente o usuario a la información contenida en la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente (un tercero que actúa en beneficio del paciente: por ejemplo, la declaración de la esposa de que el marido bebe alcohol en exceso), ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso a reserva de sus anotaciones subjetivas (artículo 18.3 LBAP).

El Decreto 29/2009, de 5 de febrero, de Galicia, por el que se regula el uso y acceso a la historia clínica electrónica, ha definido por primera vez el concepto de “anotaciones subjetivas”. En su artículo 21 entiende por tales las valoraciones personales, sustentadas o no en los datos clínicos de que se disponga en ese momento, que no formando parte de la historia clínica actual del la paciente o usuario, puedan influir en el diagnóstico y futuro tratamiento médico una vez constatadas. Añade este artículo que el personal sanitario deberá abstenerse de incluir expresiones, comentarios o datos que no tengan relación con la asistencia sanitaria del paciente o que carezcan de valor sanitario.

También puede limitarse el acceso del paciente o usuario a la información sanitaria cuando se acredite la existencia de un estado de necesidad terapéutica, es decir, cuando se entienda que el conocimiento de determinados datos de su salud puede ser gravemente perjudicial para el paciente.

En efecto, cuando en los centros, establecimientos y servicios se producen casos excepcionales en los que, por razones objetivas, el conocimiento de su situación por parte de una persona pueda perjudicar de manera grave a su salud, el médico asignado puede actuar profesionalmente sin informar antes al paciente, debiendo en todo caso informar a su representante legal o a personas vinculadas al paciente por razones familiares o de hecho y dejar constancia razonada en la historia clínica de la necesidad terapéutica existente (artículo 5.4 LBAP). Obviamente, esta excepción ha de extenderse a los datos de la historia clínica.

4. Derecho a la cancelación de los datos de salud.

De entrada, conviene señalar que la LOPD contempla la posibilidad de que el interesado exija la rectificación o la cancelación de sus datos personales. No obstante, la legislación sanitaria contiene al respecto una regulación específica.

Dispone el artículo 17 LBAP que:

1. 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.

2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas.

Por tanto, el paciente no puede exigir la cancelación de sus datos de salud cuando pueda causarle un perjuicio o a un tercero o cuando no haya transcurrido el plazo mínimo fijado por la LBAP –cinco años-. Transcurrido ese plazo, los datos no se destruyen sino que se bloquean según dispone el artículo 16.3 LOPD, conservándose únicamente a

disposición de los Administraciones Públicas y Jueces para la atención de posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de éstas. Sólo cumplido los plazos de prescripción se procederá a su definitiva supresión.

VI. EL ACCESO A LOS DATOS DE SALUD POR PERSONAS DISTINTAS AL INTERESADO.

1. El acceso por parte de familiares.

De entrada, los familiares no tienen derecho de acceso a la historia del paciente salvo consentimiento expreso de este. Cuando fallezca el paciente podrán acceder salvo expresa prohibición del mismo.

Se ha de entender por familiar la pareja, hijos, padres y hermanos. Por el contrario, a los tíos, primos, etc., salvo excepciones, se les ha de dar la consideración de terceros más que la de familiares.

En todo caso, el acceso de un familiar a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. Colisionan aquí dos derechos: el derecho del titular de la historia clínica a la intimidad de sus datos de salud y el derecho a la integridad física de quien, estando su salud en riesgo, precisa del conocimiento de cierta información contenida en la historia clínica de otra persona y que puede ser decisiva para su diagnóstico y tratamiento. Problema realmente difícil de resolver en la práctica por lo parca que ha sido la LBAP al respecto.

Y, en efecto, en el ámbito familiar, con frecuencia, se plantean problemas de difícil resolución. Como muestra, cabe traer a colación los test genéticos. Es el caso, por ejemplo, de una paciente que se ha sometido a un test genético para conocer su predisposición a sufrir un cáncer de mama. Si resulta positivo significa que los familiares también tienen esa predisposición. Entonces, el dilema de los médicos es si deben informar a los familiares de esa circunstancia a fin de prevenir esa enfermedad o si debe prevalecer el derecho de la paciente a la protección de sus datos si se niega a que se facilite ese dato. Las posiciones son encontradas. Un sector defiende que debe facilitarse la información a los familiares pues prevalece el derecho a la vida sobre el derecho a la intimidad, y

otro sector considera que debe ocultarse esa información a los familiares si no la consiente el paciente.

2. El acceso por parte de terceros o del público en general.

El artículo 11.1 LOPD establece que los datos de carácter personal objeto de tratamiento solo pueden ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. No obstante, puntualiza este artículo en su apartado 2 f) que no será necesario el consentimiento cuando la cesión de datos de salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar estudios epidemiológicos conforme disponga la legislación sanitaria. Así, el artículo 6 de la LBAP reconoce el derecho de los ciudadanos a la información epidemiológica. Lógicamente, los datos se disocian.

En lo que hace a personajes de relieve público, según doctrina del TC la libertad de información prevalece sobre la intimidad personal siempre que la comunicación a la opinión pública esté justificada por razón de interés público. La doctrina jurídica del TC y del Supremo define como personas públicas a aquéllas de "*relevancia social e interés informativo*". Incluso el Tribunal Europeo de Derechos Humanos mantiene el criterio de "que sobre los hechos que tienen interés público prima el derecho de la información sobre el del honor y que son personajes que tienen que soportar un plus de intromisión en su vida privada"⁷.

3. El acceso por facultativos sanitarios.

La LBAP reconoce el derecho a acceder a la información contenida en las historias clínicas, sin necesidad de consentimiento del paciente, a los profesionales asistenciales que realicen el diagnóstico y el tratamiento (art. 16.1)

⁷ Resultaría interesante estudiar el caso de un político que ejerce un cargo público, que padece una adicción severa o se le diagnostica una enfermedad mental invalidante, lo que puede interferir claramente en su capacidad para gobernar. ¿Es razón suficiente para hacer públicos esos datos?

El acceso a la historia clínica de los médicos internos residentes o alumnos de grado de titulaciones sanitarias, adscritos en período de formación reglada a un centro del sistema sanitario público, con finalidad docente, requiere la autorización de la dirección del centro sanitario a propuesta motivada de la persona tutora responsable de su formación.

No obstante, en la historia clínica, particularmente en la electrónica, cabe establecer determinadas restricciones a los propios facultativos sanitarios, en el sentido de sólo poder acceder a los datos clínicos necesarios para el diagnóstico y tratamiento. Por ejemplo, el conocimiento de que el feto de una mujer embarazada sea fruto de un óvulo donado es clave para el obstetra, pero es irrelevante para cualquier otro profesional (traumatólogo ante un esguince de tobillo), y es una información muy sensible para la mujer.

4. El acceso por personal de enfermería, trabajadores sociales, etc.

Ha de permitirse el acceso a la información contenida en la historia clínica al personal de enfermería, auxiliar de clínica, trabajadores sociales, a fin de garantizar una asistencia al paciente (artículo 16.1 LBAP)⁸.

El acceso debe estar restringido a los datos imprescindibles para el ejercicio de sus funciones en relación con su puesto de trabajo. Rige aquí el principio de proporcionalidad. Es recomendable que se fijen perfiles de acceso para cada profesional según su titulación y funciones de forma que sólo accedan a los necesarios para realizar las funciones que le son propias.

5. El acceso por profesionales sanitarios de centros, servicios y establecimientos concertados para la prestación de servicios.

También se debe permitir el acceso a la información contenida en la historia clínica a los profesionales sanitarios que trabajen para las personas físicas o jurídicas que presten servicios concertados en otros centros sanitarios o de Servicios Sociales de la Administración de la Comunidad Fo-

ral, previa acreditación del cumplimiento de las exigencias contenidas en la normativa de protección de datos personales. Este acceso estará limitado a las historias clínicas de los pacientes o usuario que los centros públicos remitan a los centros concertados y en el marco temporal que dure esa atención.

Estos centros concertados deben incorporar a la historia clínica electrónica la documentación clínica generada por la asistencia sanitaria prestada.

6. El acceso a efectos de las actividades de inspección, evaluación, acreditación y planificación sanitaria.

Ha de permitirse el acceso a la información contenida en la historia clínica al personal debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, en la medida en que lo precise para el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, del respeto de los derechos del paciente o de cualquier otro deber del centro en relación con los pacientes y usuarios o la propia Administración sanitaria o de servicios sociales. El acceso mencionado tiene el alcance propio de la labor encomendada a la autoridad que accede, y debe respetar el derecho a la intimidad personal y familiar de los pacientes o usuarios.

Disociación de datos. El acceso a la información contenida en la historia clínica con fines de evaluación, acreditación y planificación sanitaria obliga a preservar los datos de identificación personal del la paciente o usuario, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, excepto que el propio paciente o usuario diese su consentimiento para no separarlos.

7. El acceso a requerimiento Judicial, de la Fiscalía, del Defensor del Pueblo y de las Fuerzas y Cuerpos de Seguridad.

Ha de facilitarse siempre el acceso a la información contenida en la historia clínica del paciente o usuario para una investigación judicial o para una investigación del Defensor del Pueblo (artículo 11.2 LOPD). Cuando la autoridad judicial o el

⁸ En este sentido, informe 656/2008 de la Agencia Española de Protección de Datos.

Defensor del Pueblo lo consideren imprescindible y así lo solicite, se facilitará la información completa de la historia clínica con la unificación de los datos identificativos y los clínico-asistenciales. En el resto de los supuestos, la información quedará limitada estrictamente para los fines específicos de cada caso (artículo 22.2 y 3 LOPD).

Incluso, sin necesidad de requerimiento judicial, debe ponerse en conocimiento del juzgado o Ministerio Fiscal los pacientes atendidos por agresiones y los casos sospechosos de abusos, incluso aunque éste no lo quiera. Y al respecto, recordemos que, según dispone el artículo 16.3 LOPD, los datos de salud, aunque hayan pasado los cinco años de conservación que exige la LBAP, han de seguir conservándose, si bien bloqueados, a disposición de las Administraciones Públicas y Jueces, para la atención de posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de éstas. Sólo cumplido los plazos de prescripción se procederá a su definitiva supresión.

Los Tribunales Eclesiásticos no son órganos Integrados en el Poder Judicial a los efectos del artículo 11.2 LOPD, por lo que no puede cedérselos datos personales sin consentimiento del afectado⁹.

8. El acceso a efectos de responsabilidad patrimonial.

En los supuestos de procedimientos administrativos de exigencia de responsabilidad patrimonial sobre la asistencia sanitaria debe permitirse que los órganos administrativos competentes para su tramitación y resolución tengan acceso a la información contenida en la historia clínica del reclamante, limitado estrictamente a los fines específicos de cada caso. Así lo prevé el artículo 16.3 de la LOPD.

9. El acceso a efectos de funciones administrativas del centro, facturación de servicios sanitarios, etc.

Autoriza el artículo 16.4 LBAP que el personal de administración y gestión de los centros sanita-

rios pueda acceder a los datos de salud relacionados con sus propias funciones.

A las compañías de aseguramiento privado sólo se les debe facilitar aquellos datos de la historia clínica imprescindibles a efectos de facturación, con la finalidad de la justificación del gasto (accidentes de circulación, etc.). Cualquier otra información clínica solicitada por la compañía aseguradora requerirá el consentimiento expreso del paciente.

10. El acceso a datos de personas fallecidas.

Ya he dicho que, conforme dispone el Reglamento de la LOPD, el régimen de protección de datos de la LOPD no es de aplicación a los datos referidos a personas fallecidas. Esto trae causa de que en el derecho civil la personalidad de las personas físicas se extingue con la muerte¹⁰. No obstante, el Reglamento de la LOPD admite que las personas vinculadas al fallecido, por razones familiares o análogas, puedan dirigirse a los responsables de los ficheros o tratamientos para notificar la muerte y, tras la acreditación suficiente, pedir la cancelación de los datos.

Sin embargo, en el ámbito de los datos de salud hay que estar a lo que dispone la LBAP. Así, establece el artículo 18.4 que los familiares o personas vinculadas por análoga relación pueden acceder a los datos de la historia clínica del fallecido únicamente si éste no lo hubiera prohibido de forma expresa. Aun no existiendo prohibición expresa, tampoco pueden acceder en tres casos: a) información que afecte a la intimidad del fallecido; b) la que se refiera a las anotaciones subjetivas de los profesionales; c) la que perjudique a terceros.

11. El acceso con fines históricos, estadísticos y científicos, así como epidemiológicos, de salud pública y de investigación.

El acceso a la información contenida en la historia clínica con fines epidemiológicos¹¹, de salud pública, de investigación o de docencia se rige por lo dispuesto en la LOPD, en la Ley 14/1986, de 25

¹⁰ La STC 2000/292, de 30 de mayo, así lo contempla también.

¹¹ Por Real Decreto 2210/1995, de 28 de diciembre, se crea la Red Nacional de Vigilancia Epidemiológica.

⁹ En este mismo sentido, informe 611/2008 de la Agencia Española de Protección de Datos.

de abril, General de Sanidad, y demás normas de aplicación en cada caso, entre otras, la Ley 12/1989, de 9 de mayo, de la función estadística pública, la Ley 13/1986, de 14 de abril, de investigación científica y tecnológica y la Ley 14/2007, de 3 de julio, de investigación biomédica.

Necesaria disociación de los datos. El acceso a la información contenida en la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente o usuario, separados de los de carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato, excepto que el propio paciente o usuario diese su consentimiento para no separarlos, o bien existan criterios técnicos y/o científicos que requieran la identificación de la persona a efectos epidemiológicos y de salud pública. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos en cada caso.

No obstante, en el ámbito de la salud pública en determinados casos no cabe disociar los datos. Es el caso de las enfermedades de declaración obligatoria individual, no numérica (enfermedades infectocontagiosas)¹².

El acceso a la información contenida en la historia clínica con fines de investigación se puede llevar a cabo únicamente para proyectos de investigación que sean científicamente aprobados. Esta aprobación normalmente se efectúa por el órgano de la Consejería de Salud competente en materia de investigación y a propuesta de la dirección del

¹² La Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, habilita directamente a las autoridades sanitarias de las distintas Administraciones Públicas para el reconocimiento, tratamiento, hospitalización o control de personas cuando se aprecie indicios racionales que permitan suponer la existencia de peligro para la salud de la población debido a la situación sanitaria concreta de una persona o grupo de personas o por las condiciones sanitarias en que se desarrolle una actividad.

Sin embargo, en estos casos el derecho a la intimidad y a la confidencialidad de los datos sanitarios con el correlativo deber de su protección no está debidamente garantizado. Se hace preciso regular adecuadamente lo relativo a la confidencialidad y protección de los datos de salud de las personas implicadas en tratamientos obligatorios por padecer enfermedades transmisibles (más cuando socialmente se siguen considerando vergonzantes). La regulación de la LOPD y de la LBAP son claramente insuficientes y no dan respuesta adecuada a estas especificidades propias del ámbito sanitario.

centro al que pertenece el investigador principal del proyecto¹³.

Al objeto de garantizar la confidencialidad de la información clínica, a efectos de su difusión o publicación se han de tener en cuenta necesariamente las siguientes normas:

a) No se difundirán aquellos datos que permitan la identificación del paciente o usuario.

b) Cuando sea absolutamente necesario identificar al paciente o usuario, será preceptiva la autorización por escrito del mismo.

c) La difusión o publicación de resultados seguirá en todo caso las normas y sugerencias relativas a la buena práctica en investigación.

d) Cuando sea necesaria la publicación de imágenes médicas o cualquier otro soporte audiovisual que muestren partes del cuerpo del paciente o usuario, y de ellas se pudiera llegar a conocer su identidad, será obligatorio el permiso escrito del mismo.

VII. LOS DATOS DE SALUD DEL MENOR DE EDAD. PECULIARIDADES.

La LBAP prevé tres niveles de madurez en los menores de edad conforme a la legislación civil (menores de 18 años). En el caso de personas con 16 años se les reconoce plena capacidad y no cabe el consentimiento por representación (mayoría de edad sanitaria). Entre los 12 años y los 16 se estará al criterio de capacidad natural (madurez intelectual y emocional), presumiéndose la madurez en los que han cumplido 14 años. Por debajo de los 12 años es siempre necesaria la conformidad de los padres o tutores. El artículo 9.3.c), in fine, dispone que sólo en caso de actuación de grave riesgo en el menor maduro, según el criterio del facultativo, se informará a los padres y su opinión será tenida en cuenta.

El Convenio de 4 de abril de 1997 para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la biología y la medicina, hecho en Oviedo y ratifica-

¹³ Por Orden Foral de 31 de octubre de 1991 se creó la Comisión Asesora Técnica en materia de Investigación de ciencias de la salud.

do por instrumento de 23 de julio de 1999, en su artículo 6.2 establece que *“La opinión del menor será tomada en consideración como un factor que será tanto más determinante en función de su edad y su grado de madurez.”*

La Ley Foral 11/2002 es más explícita y en su artículo 8.2 b) dispone que *“Los menores emancipados y los adolescentes de más de dieciséis años deberán dar personalmente su consentimiento. En el caso de los menores, el consentimiento debe darlo su representante después de haber escuchado su opinión, en todo caso, si es mayor de doce años.”*

Por su parte, la LOPD apuesta por llevar hasta sus últimas consecuencias la previsión contenida en la Ley Orgánica 1/1996, de 8 de enero, sobre protección jurídica del menor, haciéndole titular de su derecho al acceso y a consentir de forma autónoma el tratamiento de sus datos a partir de los 14 años (artículo 13 del Reglamento de la LOPD), criterio éste tradicionalmente sustentado por la AEPD también en relación con el derecho de acceso a la historia clínica (Informe 409/2004).

Y es que, en el ámbito de la protección de datos personales se ha interpretado tradicionalmente que los mayores de catorce años tiene madurez suficiente para otorgar su consentimiento para el tratamiento de sus datos personales, así como para ejercitar derechos¹⁴.

En efecto, establece el artículo 13 del Reglamento de la LOPD sobre el consentimiento para el tratamiento de datos de menores de edad lo siguiente:

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

(...)

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a

los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Sin embargo, esta interpretación no es pacífica. También se postula el derecho de los padres a conocer para poder ejercer correctamente sus obligaciones.

Veamos dos ejemplos de la interpretación contraria.

El Fiscal de menores del Tribunal Superior de Justicia de Castilla-La Mancha, en el XVI Congreso de la Sociedad Española de Medicina de Adolescentes, declaró¹⁵ que *“el médico no puede ocultar información clínica a los padres de un menor que no ha cumplido dieciséis años y si actúa así sin el conocimiento y consentimiento de ellos, aunque sea a petición del menor, incumple la ley y su actuación incurre en responsabilidad.”*

El nuevo Código de Deontología de Médicos de Cataluña, alineándose con la constatada tendencia doctrinal y legal, en su artículo 33 estableció que *“El médico, en caso de tratar a un paciente menor de edad y cuando lo considere con las suficientes condiciones de madurez, deberá respetar la confidencialidad hacia los padres o tutores y hacer prevalecer la voluntad del menor.”* Pues bien, un conjunto de 112 médicos interpuso recurso contencioso-administrativo contra este artículo y el Juzgado de lo Contencioso-Administrativo núm. 12 de Barcelona, en Sentencia de 17 de septiembre de 2007, núm. 251/2007, lo ha anulado en base a dos argumentos:

a) La formulación del artículo 33, defensor de la confidencialidad de la información sanitaria del menor maduro y de su capacidad de tomar decisiones, va más allá de lo que prevé la misma norma legal que sustenta el derecho del menor (LBAP). Esta norma establece unos límites y matices que la norma deontológica no formula, en un redactado

¹⁴ En este mismo sentido, informe 409/2004 de la Agencia Española de Protección de datos.

¹⁵ Véase Diario Médico de 27 de abril de 2005.

excesivamente genérico, que habla de “madurez” en lugar de referirse a “capacidad intelectual y emocional”, como hace la Ley, y que afirma el deber de respetar la decisión de la menor en caso de aborto, cuando la LBAP exige la mayoría de edad.

b) El artículo 33 va contra el ejercicio de la patria potestad, en tanto que ésta “no debe interpretarse sólo como un conjunto de deberes tutelares sino también como un derecho de los padres sobre su descendencia, de proyectar en sus hijos su propia personalidad, sus valores, sus creencias y su cultura...”

Esta Sentencia es apelable y entiendo que está apelada ante la Sala de los Contencioso-Administrativo del Tribunal Superior de Justicia de Cataluña. Que yo sepa, todavía no ha recaído Sentencia.

La doctrina en general¹⁶, posición en la que personalmente también me sitúo, no comparte el criterio del Fiscal de menores y del Juez de Barcelona. Conforme a la legislación aplicable ya citada basta con que el menor de edad sea capaz de entender intelectualmente y emocionalmente para que sea él, y nadir más que él, quien deba ser informado y consentir el acceso a sus datos por sus padres.

El anulado artículo 33 es correcto pues no vulnera ni violenta la LBAP, que reconoce explícitamente la autonomía del menor de 16 años con juicio natural suficiente. Valorar la madurez de un menor precisamente implica analizar su capacidad intelectual y emocional. Sin embargo, la Sentencia llega a afirmar que “el médico no es nadie para valorar la madurez del menor”. Y no sólo no la violenta sino que está en plena armonía con la misma. Si al Juez no le gusta esto lo que, en todo caso, tendría que hacer es plantear cuestión de inconstitucionalidad de los respectivos preceptos de la LBAP antes de hacer una interpretación for-

zada de la misma al objeto de anular el artículo 33. En definitiva, si la LBAP reconoce al menor de 16 años maduro la “mayoría de edad sanitaria”, prevalecerá el derecho del menor a decidir que no se informe a sus padres sobre el derecho de los padres a ejercer la patria potestad y a pedir y recibir información sanitaria. La prevalencia que la Sentencia da a la patria potestad implica un menosprecio de los derechos personales de los hijos reconocidos por abundante legislación nacional e internacional. Entiendo que la “patria potestad” no implica un “derecho absoluto” de los padres o tutores a imponer a los hijos menores un comportamiento determinado.

Como acertadamente apunta DE LAMA AY-MÁ¹⁷ lo habitual es que el menor maduro permita que se informe a los padres, pero el problema se presenta cuando el menor maduro se opone expresamente a que se comunique su situación médica a sus padres. Entonces, si no se respeta su opción, además de vulnerarse la normativa aplicable, puede resultar seriamente perjudicial para el menor en la medida en que puede mostrarse reticente o contrario a acudir al médico y a revelarle la información necesaria para el tratamiento ante el temor de que se informe a los padres (temas como relaciones sexuales, enfermedades venéreas, drogas, etc.). En estos casos, no cabe duda de que, no ya desde un punto de vista jurídico, sino médico-sanitario, debe prevalecer la confidencialidad por ser más beneficioso para el menor¹⁸. Únicamente estará justificado no respetar el derecho a la confidencialidad del menor maduro cuando sea legalmente necesario el doble consentimiento o cuando el menor actúe poniendo en grave riesgo su salud (artículo 9.3.c LBAP) de una forma un tanto irrazonable, lo que, además, hará dudar seriamente de que realmente tenga el grado de madurez necesario.

¹⁶ Véase, por toda, “Documento sobre salud sexual y reproductiva en la adolescencia” elaborado por el Grupo de Opinión del Observatori de Bioètica i Dret, Barcelona, 2002, pp. 14 y 15 y A: DE LAMA AY-MÁ “La confidencialidad en el ámbito médico; aspectos problemáticos del deber de secreto en la interrupción del embarazo de una menor de edad.”, InDret. Revista para el Análisis del Derecho, núm. 2/2006, pp. 12 y 13, así como los autores citados en el trabajo, y R. URIESTE UGARTE, en Diario Médico de 10 de abril de 2006.

¹⁷ “La confidencialidad en el ámbito médico; aspectos problemáticos del deber de secreto en la interrupción del embarazo de una menor de edad.”, InDret. Revista para el Análisis del Derecho, núm. 2/2006, p. 10.

¹⁸ Esta es también la opinión plasmada en el “Documento sobre salud sexual y reproductiva en la adolescencia” elaborado por el Grupo de Opinión del Observatori de Bioètica i Dret, Barcelona, 2002, p.9.