

**INFORME “El tiempo de los derechos”, núm.14.**

# **HURI-AGE**

## **Consolider-Ingenio 2010**

### **HISTORIA CLÍNICA Y PROTECCIÓN DE DATOS PERSONALES: RECOMENDACIONES Y PROPUESTAS EN TORNO AL USO DE LA INFORMACIÓN**

INFORME ELABORADO EN EL MARCO DEL LABORATORIO DE LA *SOCIEDAD DE LA INFORMACIÓN Y DERECHOS HUMANOS* DENTRO DEL PROGRAMA “EL TIEMPO DE LOS DERECHOS”, CONSOLIDER-INGENIO 2010, POR EL GRUPO DE INVESTIGACIÓN HI13 DE LA UNIVERSIDAD DE VIGO.

#### **EQUIPO DE INVESTIGACIÓN**

##### **Dirección y Coordinación del Grupo HI13:**

Dirección: Ana Garriga Domínguez. Universidad de Vigo.

Coordinación: Susana Álvarez González. Universidad de Vigo.

**Investigadores del Grupo HI13:** Ana Garriga Domínguez, José Feijóo Miranda, Roberto O. Bustillo Bolado y Susana Álvarez González

**Colaboradores:** Mónica Mourelo Pérez.

**Noviembre 2010**

## 1. CONSIDERACIONES PREVIAS: EL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES

El derecho a la protección de datos es un derecho fundamental diferente, autónomo y más amplio que el derecho a la intimidad. El derecho fundamental a la protección de datos *persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado*<sup>1</sup>. Este derecho, consagrado por el artículo 18.4 de nuestro texto constitucional da respuesta, en la nueva realidad derivada del proceso tecnológico, “a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona”: la libertad informática<sup>2</sup>. Nos encontramos, además, ante un derecho cuya finalidad última es la de proteger y garantizar el ejercicio de los derechos fundamentales de la persona de tal manera que la violación de este derecho supondría la conculcación de otros derechos fundamentales. Este carácter instrumental se extrae del propio texto constitucional que en su artículo 18.4 establece una serie de limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos de las personas<sup>3</sup>.

Este derecho tiene por objeto, según establece el artículo 1 de la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)*<sup>4</sup> “garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”. En la redacción de este precepto influyó la Directiva 95/46/CE que dispone que su primer objetivo será la protección de los derechos y libertades de las personas físicas, siguiendo la tradición marcada por el Convenio de 28 de enero de 1981 del Consejo de Europa y también por otras normas de protección de datos personales anteriores<sup>5</sup>, cuya aprobación responde a la necesidad de proteger los derechos fundamentales de las personas en lo que respecta al tratamiento de sus datos personales.

El objeto de protección del derecho a la protección de datos personales se extenderá “a cualquier tipo de dato personal, sea íntimo o no, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos”<sup>6</sup>. Por tanto, esta protección se extenderá también a los datos públicos que, aún siendo accesibles al conocimiento de cualquiera, “no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos”<sup>7</sup>. Es decir, los datos amparados son todos aquellos que identifiquen o permitan la identificación de una persona. Así, de conformidad con el artículo 3.a), de la LOPD, habrá que entender por dato personal “cualquier información concerniente a personas físicas identificadas o identificables” y según el artículo 5.f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el

---

<sup>1</sup> Vid. STC 192/2000, de 30 de noviembre.

<sup>2</sup> *Ibidem*.

<sup>3</sup> Vid. GARRIGA DOMÍNGUEZ, A.: *Tratamiento de datos personales y derechos fundamentales*, 2ª ed., Dykinson, Madrid, 2009.

<sup>4</sup> BOE núm. 298, de 14 de diciembre.

<sup>5</sup> Vid. PÉREZ LUÑO, A. E.: “Los derechos humanos en la sociedad tecnológica”, en LOSANO, M. y otros: *Libertad informática y leyes de protección de datos*, Centro de Estudios Constitucionales, Madrid, 1990.

<sup>6</sup> Vid. STC 192/2000, de 30 de noviembre.

<sup>7</sup> *Ibidem*.

Reglamento de desarrollo de la citada Ley, “cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”. Según el apartado o) de este mismo artículo, persona identificable es “toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados”.

Si descendemos al plano de la protección de datos de carácter personal en el ámbito sanitario, se presenta como necesario realizar una especial referencia a las denominadas “informaciones sensibles” que son aquellas que se refieren a cuestiones íntimamente ligadas al núcleo de la personalidad y de la dignidad humana de tal modo que las posibles agresiones a la dignidad, libertad, las posibilidades de ser discriminado o cualquier otra contra el ejercicio de los derechos fundamentales de las personas, se van a ver agravadas. Es por ello que estos datos personales serán objeto de un reforzamiento de las medidas adoptadas para su garantía y protección. En este sentido, el artículo 7 LOPDP reúne en tres grupos o categorías de datos que, por diversas razones, exigen una protección máxima debido a lo directamente comprometidas que se hallarían la dignidad y libertad de las personas por su uso ilegítimo. Estos datos sensibles serían, en primer lugar, “las informaciones que revelen la ideología, afiliación sindical, religión y creencias”. En segundo lugar, “los datos relativos al origen racial, a la salud y la vida sexual”. Finalmente, “aquellos que hacen referencia a la comisión de infracciones penales o administrativas”. Los datos pertenecientes a la segunda categoría “sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente”. Se pueden definir los datos relativos a la salud como cualquier tipo de información concerniente a la salud pasada, presente y futura, física o mental de un individuo<sup>8</sup>.

Por otra parte, cabe señalar que en sede sanitaria nos encontramos con un problema añadido: la implantación del sistema de historia clínica electrónica. El tradicional sistema manual o de historias en papel plantea diversos inconvenientes tales como el desorden, la ilegibilidad o, incluso, la posibilidad de pérdida de algún documento. Por ello, la informatización de la historia clínica ha supuesto un gran avance no sólo por el hecho de que da solución a muchos de estos problemas sino también porque permite integrar toda la información relativa a un paciente en una única historia clínica lo cual facilita la tarea de los profesionales sanitarios. Ahora bien, el empleo de esta técnica plantea graves inconvenientes como pueden ser la capacidad de almacenamiento limitada de los equipos informáticos, la falta de adaptación del personal y, sobre todo, desde el punto de vista de la protección de datos de carácter personal, los accesos no autorizados. El problema no reside tanto en la cantidad de información que es posible recabar sino en la posibilidad de vincular y tratar esa

---

<sup>8</sup> Dentro de la categoría de datos médicos, la Recomendación (97) 5, adoptada el 13 de febrero de 1997 por el comité de Ministros del Consejo de Europa incluye también los datos genéticos. Así, establece el artículo 5 del Reglamento de desarrollo de la LOPDP que son “datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética”. Sobre esta cuestión vid. ÁLVAREZ GONZÁLEZ, S.: Derechos fundamentales y protección de datos genéticos, Dykinson, Madrid, 2007.

información y obtener perfiles de la personalidad en función de los cuales se pueden adoptar decisiones favorables o desfavorables<sup>9</sup>.

## 2. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL ÁMBITO SANITARIO

En materia de protección de datos en el ámbito sanitario ha de tenerse en cuenta lo dispuesto en la *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*<sup>10</sup> (Ley 41/2002) que establece, por una parte, la obligación de información y de documentación clínica de todo profesional que interviene en la actividad asistencial (artículo 2.3) y, por otra, el correlativo derecho de todo paciente o usuario 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 la atención primaria como de atención especializada (artículo 15.1). De este modo, el soporte de los datos relativos a la salud es la historia clínica que es un fichero en el que se almacenan tanto datos individuales del paciente como aportaciones de los profesionales sanitarios<sup>11</sup>. En este sentido, podemos afirmar que la historia clínica es el soporte de los datos relativos a la salud y es definida por la Ley 41/2002 como “el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y evolución clínica de un paciente a lo largo del proceso asistencial” (artículo 3). Por otra parte, establece el artículo 14 de esta misma norma que “la historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro”. Documentación clínica es “el soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial” (artículo 3). Estos conceptos encajan en la definición de fichero del artículo 3 LOPDP que lo considera como un conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

La historia clínica, por tanto, puede considerarse como el soporte, informatizado o no, que contiene la información clínica del sujeto. En consecuencia, los datos relativos a la salud que forman parte de la historia clínica van a constituir parte de un fichero informático o manual estructurado que va a estar conformado por el conjunto de historias clínicas de cada centro asistencial<sup>12</sup>. Así, la Ley 41/2002 recoge la creación y la existencia de la historia clínica como un derecho del paciente y como un deber por parte del centro o institución sanitaria (artículos 15 y 14.2).

---

<sup>9</sup> Vid. GARRIGA DOMÍNGUEZ, A.: *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2004, pp. 24 y ss.

Estos perfiles de la personalidad vinculados a unos datos relativos a la mala salud de un paciente pueden convertirse en auténticas “listas negras”. Vid. SÁNCHEZ BRAVO, A.: *La protección del derecho a la libertad informática en la Unión Europea*, Universidad de Sevilla, Sevilla, 1998, p. 106.

<sup>10</sup> BOE núm. 274, de 15 de noviembre.

<sup>11</sup> La LOPDP define el fichero como “todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso” [artículo 3.b)].

<sup>12</sup> Recomendación 2/2004 de 30 de julio, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre custodia, archivo, seguridad de los datos de carácter personal de las historias clínicas no informatizadas. Boletín Oficial de la Comunidad de Madrid núm. 191, de 12 de agosto de 2004.

El artículo 15 de la Ley 41/2002 recoge el contenido de la historia clínica al indicar, en primer lugar, las condiciones que han de presidir la elaboración de dicho contenido en los siguientes términos: “la historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente”. Ésta tendrá como finalidad principal la de facilitar la asistencia sanitaria, dejando constancia de todos los datos que permitan conocer el estado de salud de una persona (artículo 15.2). Asimismo, se recoge la aplicación de los principios de calidad de los datos, regulados en el artículo 4 LOPDP, a la recogida y tratamiento de información en el ámbito sanitario<sup>13</sup>, pues como señala Lucas Murillo de la Cueva, en relación con el tratamiento jurídico de los documentos y registros sanitarios, será necesario volver en todas las ocasiones que sea preciso a los principios del derecho a la protección de datos, “y en particular a sus reglas básicas”<sup>14</sup>.

La Ley Orgánica 15/1999 intenta identificar los riesgos que para los derechos de las personas suponen el tratamiento de sus datos personales y al mismo tiempo garantizar los intereses legítimos, públicos o privados que justifiquen ese tratamiento. Así, el artículo 4 de esta norma regula la calidad de los datos estableciendo los principios básicos que deberán respetarse en la recogida, tratamiento, uso y almacenamiento de los datos personales, de manera que sólo tendrán una calidad adecuada aquellos respecto de los cuales se cumplan estos principios. Se trata de normas que regulan la recogida, registro y uso de los datos personales y están encaminadas a garantizar tanto la veracidad de la información contenida en los mismos, como la congruencia y racionalidad de su utilización. Estos principios, que tienen su reflejo en el ámbito sanitario a través de la Ley 41/2002, son los siguientes:

1. Principio de pertinencia: este principio exige que los datos personales estén relacionados con el fin perseguido por lo que deberán ser “*adecuados y no excederán de las finalidades para las que se hayan registrado*”<sup>15</sup>.

2. Principio de finalidad: sólo se podrán recoger y tratar los datos personales que “sean adecuados (...) en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido”. Además, los datos personales objeto de tratamiento “no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos” (artículo 4, apartados 1 y 2 LOPDP). Asimismo, los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados” (artículo 4.5 LOPDP).

La historia clínica tiene como finalidad principal la de archivar y recoger los datos del paciente necesarios para la asistencia sanitaria, tanto para el cuidado de su

---

<sup>13</sup> Se trata de una especificación de los principios de pertinencia, finalidad, veracidad y exactitud aplicados a la recogida de la información contenida en la historia clínica, por lo que los datos que en ella figuren serán adecuados e imprescindibles para la finalidad principal perseguida por la norma, esto es, facilitar la asistencia sanitaria en cada ámbito concreto y determinado.

<sup>14</sup> MURILLO DE LA CUEVA, P.: “El tratamiento jurídico de los documentos y registros sanitarios informatizados y no informatizados”, en *Información y Documentación Clínica*, Vol. II, Consejo General del Poder Judicial, Ministerio de Sanidad y Consumo, Madrid, 1997, p. 589.

<sup>15</sup> PÉREZ LUÑO, A. E.: “Los derechos humanos en la sociedad tecnológica”, en LOSANO, M. y otros: *Libertad informática y leyes de protección de datos*, Centro de Estudios Constitucionales, Madrid, 1990, p. 166.

salud en el presente como en el futuro. Por consiguiente, todos los datos que figuren en la historia clínica deben ir encaminados a esta finalidad. Dicha función ha sido recogida por el artículo 16, apartado primero, de la Ley 41/2002 que señala: “la historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia”. Se pueden señalar otros usos de la historia clínica, si bien estos quedarán subordinados al éste. Así, al margen de la asistencia sanitaria, el artículo 16.3 permite la utilización de los datos contenidos en la historia clínica para finalidades judiciales, epidemiológicas, de salud pública, de investigación y de docencia. Para el empleo de estos datos con estas finalidades será necesario el cumplimiento de una serie de requisitos. En primer lugar, preservación de la identidad del sujeto mediante la separación de los datos de identificación de las informaciones de carácter clínico-asistencial, con la finalidad de garantizar el anonimato, salvo consentimiento de la persona para que aparezcan unidas esas informaciones y salvo los supuestos de investigación por parte de la autoridad judicial en los que sea preciso la relación entre la identidad del sujeto y los datos relativos a su salud. En segundo lugar, la adecuación entre los datos y documentos a los que se pretende acceder y la finalidad para la cual van a ser utilizados. Ambos requisitos han de darse de forma conjunta.

3. Principio de veracidad y de exactitud: el artículo 4.3 de la LOPDP exige que los datos sean “exactos y puestos al día de forma que respondan con veracidad a la situación del afectado”. Así, corresponderá al responsable del fichero adoptar los mecanismos y prevenciones necesarios para garantizar la adecuación a la realidad de los datos registrados, empleando el nivel de diligencia exigible para garantizar la veracidad de éstos.

En este sentido, el artículo 15.2 de la Ley 41/2002 exige que en la historia clínica consten todos aquellos datos que permitan el conocimiento veraz y actualizado del estado de salud del paciente. Asimismo, regula en el artículo 2.5 la obligación del paciente de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria, pues, los derechos a la intimidad, al respeto de su dignidad, a la confidencialidad de la información y a acceder a sus datos sanitarios tienen como contrapartida esta obligación de los pacientes y usuarios de los servicios sanitarios de facilitar los datos sobre su estado físico y de salud, de manera leal y verdadera colaborando en su obtención en esos casos.

4. Principio de lealtad: los datos personales han de obtenerse sin engaños o falsedades por parte de quien los solicita, prohibiéndose de forma contundente la utilización de medios fraudulentos, desleales o ilícitos (artículo 4 LOPDP).

5. Principio de seguridad de los datos: la LOPDP obliga a que se adopten las medidas necesarias para garantizar la seguridad de los datos personales evitando su alteración, pérdida, tratamiento o acceso no autorizados. Por ello, “no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se

determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas” - artículo 9.2 -<sup>16</sup>!

La Ley 41/2002, de 14 de noviembre, responsabiliza de la custodia y seguridad de las historias clínicas, y por lo tanto de los datos personales de los pacientes, a los centros sanitarios. Obliga a los centros, públicos o privados, con independencia del soporte en el que se recoja la historia clínica, a garantizar su seguridad, su correcta conservación y la recuperación de la información. Asimismo, se exige a las Administraciones sanitarias establecer los mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura y a las Comunidades Autónomas aprobar las disposiciones necesarias “para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental” - artículo 14.4 -. El artículo 19 de esta misma Ley refuerza esta obligación al garantizar el derecho del paciente a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Esta custodia debe permitir la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad ya que para asegurar los derechos del interesado en relación con su historia clínica, especialmente lo relativo a su confidencialidad, tanto la LOPDP como la normativa sanitaria regulan el deber de secreto de los profesionales que conozcan las informaciones personales allí recogidas. Por otra parte, establece el artículo 10 de esta Ley la obligación para el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de datos de carácter personal de respetar el secreto profesional respecto de los mismos y el deber de guardarlos. Además, estas obligaciones subsistirán aún después de finalizar sus relaciones con el titular del fichero o con el responsable del tratamiento, en su caso.

En el ejercicio de algunas profesiones es imprescindible que quienes las ejercen tengan acceso a información de carácter personal sobre sus clientes o personas con las que se relacionan. En algunos casos la “*información es necesaria para el ejercicio profesional (...); en otros, en cambio, la información se recibe con ocasión del ejercicio de la profesión, pero no es consustancial a la misma*”<sup>17</sup>. Todo aquel que por razón de su profesión conoce datos sobre otros con los que se relaciona, tiene un deber general de no quebrantar la confianza que ha recibido y este deber de discreción “*alcanza un grado distinto cuando la ley lo configura como un deber positivo de guardar secreto profesional*”<sup>18</sup>. Este último es el supuesto contemplado en la LOPDP, puesto que afirma el deber positivo de secreto profesional respecto de los datos de carácter personal a que tuvieren acceso, de los responsables del fichero o de quienes intervengan en cualquier fase del tratamiento de los mismos. El responsable del tratamiento o quien intervenga en alguna fase de éste se encuentra doblemente obligado cuando la información personal se refiera a la salud de las personas, ya que al deber general de secreto establecido en la Ley de Protección de Datos de Carácter Personal debe sumarse el regulado en el artículo 2.7 de la Ley 41/2002, de 14 de noviembre, que dispone que “la persona que elabore o

---

<sup>16</sup> El concepto de seguridad debe abarcar tanto la confidencialidad de la información como la disponibilidad e integridad de la misma. De este modo, las medidas de seguridad exigibles se califican en tres niveles distintos (básico, medio y alto), en función del tipo de datos personales almacenados, tanto para los ficheros tradicionales como para los automatizados.

<sup>17</sup> SAINZ MORENO, F.: “Secreto e información en el Derecho público”, en *Homenaje a García Enterría*, Volumen III, Civitas, Madrid, 1993, p. 2875.

<sup>18</sup> *Ibidem*.

tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida”. Es decir, no sólo se obliga al sigilo profesional al personal sanitario que tenga conocimiento o acceso a la información personal sobre la salud, sino a cualquiera que incluso por razones de mera gestión acceda a esos datos. En consonancia con lo establecido en el artículo 10 LOPDP, la Ley 41/2002 “no limita la obligación de secreto al médico, sino que la extiende a toda persona que en el ejercicio de sus funciones tenga conocimiento de los datos médicos de un paciente o usuario de los centros sanitarios, tanto públicos como privados”<sup>19</sup>.

Por otra parte, es necesario tener presente que el deber de secreto es general, tanto para los responsables de los ficheros de titularidad pública como para los de titularidad privada. Sin embargo, en el caso de los funcionarios públicos, el deber de secreto se ve reforzado puesto que la legislación estatal les impone “un deber de «sigilo» sobre todo aquello que conocen por razón de su cargo y un deber de «secreto» sobre las materias clasificadas o declaradas secretas por la ley”<sup>20</sup>. Por último, nuestro ordenamiento refuerza la obligación de sigilo y secreto para todos aquellos que tengan conocimiento de informaciones personales por razón de su cargo, profesión u oficio, tanto en el ámbito privado como en el público, tipificando en el Título X del Código Penal la revelación de secreto. Por lo tanto, corresponderá a los centros sanitarios adoptar todas las medidas necesarias para garantizar la intimidad de las personas y la confidencialidad de la información, debiendo asimismo, elaborar las normas y procedimientos protocolizados para garantizar el acceso legal a los datos de los pacientes.

En otro orden de cosas cabe señalar que las garantías que la LOPDP establece para dotar el tratamiento de datos personales de una determinada calidad han de completarse, necesariamente, con el conjunto de facultades con las que el interesado o titular de los datos cuenta para controlar el uso de esta información. Se trataría de los derechos de información y a prestar o no el propio consentimiento - que constituyen instrumentos *a priori* de control sobre los datos personales, anteriores al momento en que éstos pasan a formar parte de un fichero - y los derechos de acceso, cancelación y rectificación - que son instrumentos de control *a posteriori*, ya que permiten a su titular ejercer el control sobre aquellos datos que han sido recabados y registrados en el pasado -. Los derechos que la ley garantiza a los interesados junto con los deberes jurídicos que la misma impone al responsable del fichero y a las demás personas que intervengan en alguna fase del tratamiento, consecuencia de aquéllos, constituyen el conjunto de instrumentos de los que la LOPDP se sirve para hacer realidad los principios de protección de datos y garantizar a las personas un control efectivo sobre sus datos personales.

1. El derecho de información. Se trata de un derecho genérico “a estar informado” y que se realiza en la LOPDP a través de una doble vía: la garantía del afectado del derecho a ser informado en el momento de la recogida de sus datos de los aspectos relativos a su tratamiento y el derecho a “conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de ficheros de datos de carácter personal, sus finalidades y la identidad del responsable del

---

<sup>19</sup> ÁLVAREZ GONZÁLEZ, S.: *La utilización de los datos genéticos por las compañías aseguradoras*, Fundación MAPFRE, Madrid, 2006, p. 67.

<sup>20</sup> SAINZ MORENO, F.: *Secreto e información en el Derecho público*, en Homenaje a García Enterría, Volumen III, Civitas, Madrid, 1993, pp. 2890 y 2891.

tratamiento” (artículo 14 LOPDP). El artículo 5 de la LOPDP establece que las personas de las que se soliciten informaciones personales deberán ser informadas, de manera previa a la recogida de los mismos y de modo expreso, preciso e inequívoco, sobre la existencia de un fichero o tratamiento de datos personales, la finalidad de su recogida y los destinatarios de la información, el carácter obligatorio o facultativo de las respuestas a las cuestiones planteadas, las consecuencias de la obtención de los datos o de la negativa a facilitarlos, la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y la identidad y dirección del responsable del tratamiento o de su representante. Asimismo, establece este precepto en su apartado 5 la obligatoriedad de informar a los interesados cuando los datos no hayan sido recabados directamente de ellos en los términos y sobre las cuestiones anteriores.

En el ámbito sanitario, este artículo 5 se completa con lo establecido por la Ley 41/2002 en relación con el derecho de información asistencial recogido en los artículos 4 y 5. Disponen la citada norma que la titularidad corresponde exclusivamente al paciente y sólo cuando consienta de manera expresa o tácita o carezca de capacidad para entender la información a causa de su estado físico o psíquico, podrá informarse a las personas a él vinculadas por razones familiares o de hecho. Este derecho puede ser limitado por la existencia acreditada de un estado de necesidad terapéutica, es decir, cuando a juicio del médico y por razones objetivas, el conocimiento de su propia situación pueda perjudicar de manera grave la salud del paciente. No obstante, dicha circunstancia deberá quedar reflejada en la historia clínica (artículo 5.4 de la Ley 41/2002).

2. El consentimiento del interesado: el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa (artículo 6.1 LOPDP)<sup>21</sup>. De este modo, es necesario señalar que es condición indispensable para que el interesado pueda prestar el consentimiento a que se refiere la Ley, el cumplimiento previo del contenido del derecho de información en la recogida de datos. Por otra parte, el artículo 11 de esta Ley limita la comunicación de los datos de carácter personal a un tercero a aquellas cesiones que cumplan dos requisitos: la autorización previa del interesado y que la comunicación se produzca en razón de fines directamente relacionados con las funciones legítimas del cedente y del cesionario. Este precepto no permite un consentimiento incondicionado y falto de requisitos, de manera que el consentimiento será nulo cuando recaiga sobre un cesionario indeterminado o indeterminable o cuando al interesado no le sea posible conocer la finalidad de la cesión que consiente.

3. Los derechos de acceso, rectificación y cancelación: son derechos subjetivos independientes, de carácter personalísimo.

El artículo 15 LOPDP configura el derecho de acceso como la facultad del individuo de solicitar y obtener gratuitamente información de sus datos personales sometidos a tratamiento, del origen de los mismos y de las comunicaciones realizadas o previstas. Su ejercicio se encuentra sometido a un límite temporal puesto que sólo podrá ejercitarse a intervalos no inferiores a doce meses, salvo que se acredite un interés legítimo que justifique un nuevo acceso. El afectado, en virtud de este derecho, podrá

---

<sup>21</sup> Art. 3 LOPDP: “consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen”.

obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero o a la totalidad de sus datos sometidos a tratamiento. Así, la Ley 41/2002 garantiza igualmente el derecho del paciente de acceso a la historia clínica. El artículo 18 de esta Ley garantiza el derecho de acceso a la documentación de la historia clínica y a la obtención de copia de los datos que figuren en ella. Este derecho puede ser ejercido por el propio paciente o por representante debidamente acreditado. Ahora bien, el acceso a los propios datos relativos a la salud recogidos en la historia clínica tiene dos limitaciones: el derecho de terceras personas a la confidencialidad de los datos que constan en la historia clínica y que fueron recogidos en interés terapéutico del paciente y el derecho de los profesionales participantes en su elaboración, quienes pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

Por otra parte, los derechos de rectificación y cancelación se regulan de forma conjunta en el artículo 16 LOPDP. Así, por un lado, el interesado tiene derecho a que los datos que figuren de manera inexacta o errónea en un fichero sean corregidos e integrados y, por otro, la facultad de eliminar de un fichero aquellos datos de carácter personal *“que no deban figurar en él, ya sea porque nunca debieron ser registrados, ya sea porque habiéndose recogido legalmente, diversas causas exigen su supresión”*<sup>22</sup>. Estos derechos suponen para el responsable del tratamiento, no sólo la obligación de rectificar o cancelar los datos personales, sino además, en caso de comunicación, el deber de notificar a quien se hayan comunicado los datos, la rectificación o cancelación efectuada sobre los datos cedidos. Por otra parte, por lo que respecta a la historia clínica, el derecho a cancelar los datos contenidos en la misma se encuentra limitado por las previsiones del artículo 17 de la Ley 41/2002, que establece un plazo de conservación de esa información de al menos cinco años desde el alta del proceso asistencial. También deberá conservarse, según este mismo precepto a efectos judiciales de conformidad con la legislación vigente y cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud.

### **3. DATOS RELATIVOS A LA SALUD CONTENIDOS EN LA HISTORIA CLÍNICA: SUS USOS LEGALES**

Como ya se ha señalado, la historia clínica constituye el soporte de los datos relativos a la salud, es decir, se trata de un fichero entendido en los términos previstos por la LOPDP. La regulación de los datos relativos a la salud en la LOPDP se encuentra, de forma genérica, en el artículo 7 LOPDP y se complementa con lo dispuesto por el artículo 8 que autoriza a las instituciones y centros sanitarios, públicos y privados, y a los profesionales correspondientes a tratar los datos relativos a la salud de las personas que acudan a ellos o hayan de ser tratados en los mismos. El artículo 8 LOPDP se completa por lo dispuesto en la *Ley 41/2002, de 14 de noviembre, Básica Reguladora de la Autonomía del Paciente*; la *Ley 14/1986, de 25 de abril, General de Sanidad*<sup>23</sup> y el Convenio del Consejo de Europa de 4 de abril de 1997 para la Protección de los Derechos Humanos y la Dignidad del Ser Humano respecto de las aplicaciones de la Biología y la Medicina (Convenio sobre los Derechos del Hombre y Biomedicina), que entró en vigor en España en enero de 2000.

---

<sup>22</sup> MURILLO DE LA CUEVA, P. L.: *Informática y protección de datos personales*, Cuadernos y Debates número 43, Centro de Estudios Constitucionales, Madrid, 1993, p. 79.

<sup>23</sup> BOE núm. 102, de 29 de abril.

La Ley General de Sanidad garantiza los derechos de los afectados al respeto de su personalidad, dignidad e intimidad y la confidencialidad de toda la información relacionada con su proceso y estancia en instituciones sanitarias, públicas o privadas. La Ley 41/2002 incluye estos mismos derechos entre sus principios básicos. Así, el Capítulo I - Principios generales - contiene las normas básicas sobre el tratamiento de la información relativa a la salud y ha de completarse con los Capítulos II - El derecho de información sanitaria - y III - El derecho a la intimidad -. Señala el artículo 2.1 que “la dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica”. Asimismo, prevé el artículo 7.1 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 otra parte, la Ley 41/2002 contiene una regulación pormenorizada de determinados aspectos de la historia clínica: el acceso a la misma, sus posibles usos y el deber de secreto de las personas que tienen acceso a ella. En primer lugar, por lo que respecta al acceso a la historia clínica, esta norma distingue el acceso de los profesionales (artículo 16) del derecho de acceso de los pacientes (artículo 18) entendido como el derecho del interesado a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos<sup>24</sup>. Establece el apartado 1 del artículo 16 que “la historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia”. Asimismo, en su apartado 4 permite el acceso del personal de administración y gestión de los centros sanitarios a los datos de la historia clínica relacionados con sus propias funciones. No se trata de un derecho genérico a conocer todos los datos que obran en la historia clínica, “*sino que el conocimiento viene determinado por la finalidad de las funciones*”<sup>25</sup>. Finalmente, el apartado 5 del artículo 16 permite el acceso al personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación. Dicho personal podrá acceder a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso - artículo 16.7 de la Ley 41/2002-.

Por otra parte, el artículo 18 de la Ley de Autonomía del Paciente regula el derecho de acceso del paciente a la historia clínica, a la documentación de la historia y a obtener copia de los datos que figuran en ella. Ahora bien, este derecho no podrá ejercitarse en perjuicio de derechos de terceras personas a la confidencialidad de los datos que constan en la historia clínica recogidos en interés terapéutico del paciente ni tampoco en perjuicio del derecho de los profesionales participantes en su elaboración

---

<sup>24</sup> Artículo 15.1 LOPDP.

<sup>25</sup> ÁLVAREZ GONZÁLEZ, S.: *Derechos fundamentales y protección de datos genéticos*, Dykinson, Madrid, 2007, p. 252.

que podrán oponer al derecho de acceso la reserva de sus anotaciones subjetivas - artículo 18.3 de la Ley 41/2002 -. Por tanto, es muy importante resaltar que el acceso a la historia clínica, incluso en los casos habilitados legalmente, deberá ajustarse a los principios de calidad y proporcionalidad. Este último supone el deber de limitar el acceso a los datos que efectivamente resulten necesarios para el cumplimiento de la finalidad que justifique dicho acceso, sin que deba extenderse a datos no vinculados a dicha finalidad.

En relación con los usos de la historia clínica, hay que tener en cuenta que los datos relativos a la salud se encuentran amparados por el principio de finalidad por lo que no podrán ser utilizados para usos distintos de los estrictamente sanitarios, es decir, para prevenir, controlar y tratar las enfermedades o epidemias, realizar investigaciones, etc. En concreto, la Ley 41/2002 establece que los usos legales de la historia clínica son los siguientes: en primer lugar, la finalidad o uso principal de los datos del paciente es garantizarle una asistencia sanitaria adecuada. En segundo lugar, establece el artículo 7.6.párrafo segundo LOPDP que los datos relativos a la salud podrán ser objeto de tratamiento cuando el mismo resulte 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. En tercer lugar, de acuerdo con el artículo 16.3 de la Ley 41/2002, se prevén otros fines o usos legales posibles que son los judiciales, epidemiológicos, de salud pública, de investigación o de docencia. Por último, se refiere el artículo 16.5 de la Ley de Autonomía del Paciente a las funciones de inspección al señalar que “el personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tendrá acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria”.

Finalmente, tal y como se ha señalado, cabe recordar que las normas anteriores se ven completadas con las obligaciones de reserva debida y secreto a las que están sujetos todos los profesionales que intervienen en la actividad asistencial (artículo 2.7 de la Ley 41/2002) y aquellos a los que se les comunican los datos de la historia clínica o acceden a ella. Igualmente se establecen obligaciones relativas al mantenimiento y conservación en condiciones de seguridad de acuerdo con lo establecido en la LOPDP. Asimismo, la Ley 15/1999 exige en su artículo 7.6 que el tratamiento de datos relativos a la salud se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta a una obligación equivalente de secreto. Es decir, cualquier profesional que acceda a la información contenida en la historia clínica está sometido al deber de secreto que quedará protegido de forma general por la normativa que protege el derecho a la intimidad<sup>26</sup>.

#### **4. RECOMENDACIONES Y PROPUESTAS**

**1.** La dignidad de la persona, el respeto a la autonomía de la voluntad del paciente y el derecho a que se respete el carácter confidencial de los datos médicos constituyen la

---

<sup>26</sup> ROMEO CASABONA, C. M.: “La intimidad del paciente desde la perspectiva del secreto médico y del acceso a la historia clínica”, en *Derecho y Salud*, Vol. 1, núm. 1, julio-diciembre, 1993, p. 5.

base que orientará necesariamente toda actividad relacionada con la obtención, archivo, custodia y transmisión de la información contenida en la historia clínica.

2. El derecho a la protección de datos actúa como mecanismo de protección de la persona frente al tratamiento de su información de carácter personal, incluido el archivo de los datos relativos a la salud. La historia clínica constituye el soporte en el que queda registrada la información médica obtenida de pacientes o usuarios de centros e instituciones sanitarias. La finalidad principal de la historia clínica es la de recoger y archivar los datos necesarios del paciente para llevar a buen término una adecuada asistencia sanitaria. **Consecuentemente, todos los datos que consten en la misma deberán ir encaminados a esta finalidad. Cualquier otro uso de los datos personales contenidos en la historia clínica ha de considerarse secundario, excepcional, restringido y subordinado al primero.**

3. La titularidad de la información médica corresponde al paciente. La regla general ha de ser el conocimiento del sujeto de la información que le concierne. **Sólo cuando consienta de manera expresa o tácita, podrá informarse a las personas vinculadas al paciente por razones familiares o de hecho. Sólo en supuestos singulares fundamentados en un interés general, recogidos legalmente, podrán establecerse excepciones a esta regla general.**

4. El secreto profesional se presenta como mecanismo esencial para salvaguardar la privacidad del paciente en relación con los datos contenidos en la historia clínica. Es necesario insistir en la idea de que dicha obligación no se limita al secreto médico. **Este deber se extiende a toda persona que en el ejercicio de sus funciones tenga conocimiento de los datos médicos de un paciente o usuario de los centros sanitarios, públicos y privados.**

4. Las garantías y límites que condicionan el tratamiento de los datos personales en el ámbito sanitario – principios de calidad de los datos – han de completarse con la atribución al sujeto de un haz de facultades positivas que permitan el control efectivo de su información.

5. Resulta necesario que la normativa preste especial atención al auge de la historia clínica electrónica, con los peligros que ello conlleva en relación con los posibles accesos no autorizados a la misma en la actual sociedad de la información. En este sentido se propone **la revisión de la legislación a fin de articular un mecanismo uniforme para el control del acceso al historial clínico al mismo tiempo que se refuerzan las garantías para la intimidad de los pacientes y para la protección de sus datos** con el objetivo de evitar la disparidad de criterios.