CONFIDENCIALIDAD Y PROTECCIÓN DE LOS DATOS DE SALUD INFORMATIZADOS

Comisión de Bioética de Castilla y León

2015

Junta de Castilla y León

COMISIÓN DE BIOÉTICA DE CASTILA Y LEÓN

Presidente:

Antonio Blanco Mercadé

Vicepresidente:

Juan Carlos Martín Escudero

Secretaria:

Mª del Carmen Cardeñosa García

Vocales:

Rufino Álamo Sanz

Carmen Bermejo Merino

Tomás Casado Gómez

Ana Mª Company Vázquez

Carmen Fernández Alonso

José Antonio Franco Yagüe

Mª Concepción García de la Villa Redondo

Mercedes González García

Mª Jesús Ladrón de San Ceferino

Alberto Orfao de Matos

Julia Rodríguez Barbero

Álvaro Sanz Rubiales

INTRODUCCIÓN

El objetivo de cualquier sistema de salud es prestar la mejor atención posible a los ciudadanos. Para ello, es fundamental disponer de un procedimiento adecuado de almacenamiento, gestión y acceso a la información sobre datos personales, especialmente sobre datos de salud, que permita una atención personal, integrada y continua. Los recursos informáticos disponibles permiten acceder a las historias clínicas y actualizarlas de forma continua, constituyendo un instrumento muy importante para la consecución de ese fin.

En el ámbito sanitario, el desarrollo de los sistemas de información donde se genera una gran cantidad de datos personales conlleva la aparición de nuevos riesgos que pueden afectar a derechos de pacientes y usuarios. Muchos de estos datos personales son especialmente sensibles y precisan por ello de una especial protección y administración. En consecuencia, los responsables de proporcionar atención sanitaria deben asumir nuevas obligaciones éticas que permitan minimizar dichos riesgos.

Hay que promover una cultura de responsabilidad en la protección y en la confidencialidad de los datos de salud durante su utilización. Por ello, por encima de las medidas requeridas por el marco jurídico vigente, debe identificarse y potenciarse un comportamiento ético auto-regulado entre los profesionales de la salud o de otros ámbitos que puedan conocer legítimamente datos de una persona. Dicho comportamiento ético ha de ir más allá de los necesarios sistemas de control al acceso, la introducción y modificación de datos, su cesión, distribución o manipulación.

En este documento, la Comisión de Bioética de Castilla y León formula una serie de consideraciones que tienen por objeto poner de manifiesto tanto los beneficios como los posibles riesgos que dichos sistemas de información tienen sobre la confidencialidad y la protección de los datos de salud almacenados y disponibles en formato electrónico.

Además, se describen algunos principios o fundamentos que podrían orientar la gestión y el uso de estos datos informatizados, y se realizan algunas recomendaciones para una utilización adecuada y responsable de los mismos, con el propósito final de mejorar la calidad asistencial sanitaria, aspirando siempre a la excelencia.

FUNDAMENTACIÓN

La información clínica debe estar a disposición de los profesionales en el ejercicio de su actividad, a través de un sistema informático moderno. Por otro lado, dichos profesionales tienen la obligación ineludible de respetar la confidencialidad de esa información. El conflicto surge cuando se enfrentan estos dos valores: accesibilidad a los datos informatizados y respeto a la confidencialidad.

En la asistencia sanitaria es frecuente que sea el propio paciente quien desvele información de su esfera íntima a los profesionales que le atienden, mediante la aportación de datos personales (de salud principalmente, pero también de otra índole) o colaborando en su obtención. Paralelamente, el mismo paciente espera de los profesionales que respeten la confidencialidad y no revelen esa información, que, no obstante, podrá ser compartida con otros profesionales cuando ello sea necesario para prestarle una mejor atención. Por eso, ***la confidencialidad de la intimidad es un derecho que se complementa con el derecho a la protección de datos de carácter personal,*** que otorga a su titular un poder de control sobre ellos, así como sobre el uso y destino de los mismos, con el fin de evitar un uso ilícito y lesivo de estos datos.

Los datos de carácter personal que se manejan con motivo de la asistencia sanitaria están considerados por la legislación vigente como ***datos especialmente sensibles, que gozan* del *nivel más alto de protección.*** Por eso, el derecho de la persona a que se respete el carácter confidencial de este tipo de datos lleva aparejada ***la obligación de no revelarlos sin el consentimiento de su titular***, salvo que acontezca alguna de las situaciones previstas en la ley que justifiquen el levantamiento de la confidencialidad porque se trate de proteger otros bienes jurídicos (la salud de terceros o de la colectividad, protección de menores o incapaces…). Este deber de guardar la debida reserva y confidencialidad de la información es lo que se conoce como ***obligación de secreto profesional***, y ***afecta a todo el personal que accede a la información, sea este personal sanitario o no sanitario***.

El deber de secreto profesional se dice que es un deber "perfecto", porque es correlativo al derecho del paciente a la confidencialidad de sus datos personales o de salud.

Para facilitar la asistencia sanitaria y para que ésta sea de calidad, la información obtenida a lo largo del proceso asistencial debe quedar registrada, ya sea en papel o en otro soporte técnico que se precise y con el que se cuente. En la actualidad se ha

generalizado el ***uso de medios informáticos para almacenar y consultar datos de salud en la asistencia***. Esta informatización de las historias clínicas, de los documentos y de los datos sanitarios, facilita su almacenamiento, conservación y acceso, así como la coordinación de la actuación sanitaria. Todo eso supone un beneficio para el paciente, para el profesional, para el personal trabajador y para la Institución sanitaria; aumenta la calidad, la seguridad, la eficiencia y la equidad de la asistencia prestada a cada paciente en particular y a la población en general.

La necesaria preservación de la confidencialidad y protección de los datos de salud informatizados, corre en la actualidad dos importantes riesgos:

- En primer lugar, la información referente a la salud de las personas es una ***información compartida por diferentes profesionales, sanitarios y no sanitarios, e incluso por diferentes instituciones, lo que puede dificultar mucho en la práctica la observancia de un respeto absoluto de la confidencialidad.***

- En segundo lugar, aunque los sistemas de informatización también pueden contribuir a que exista un mayor control de acceso a los datos clínicos y personales registrados sobre un paciente, paradójicamente también pueden generar un ***mayor riesgo de que se conozcan o se divulguen esos datos de forma no autorizada, para fines distintos de los que llevaron a su recogida, conservación y/o cesión.***

Ante esta realidad y para minimizar los riesgos ***se impone llevar a cabo un cambio cultural y de actitud, que propicie un mayor sentido personal de la responsabilidad en el acceso y uso de los datos por parte de todos los profesionales y trabajadores que tengan acceso a ellos.***

Ningún conjunto de medidas físicas de seguridad, sistemas de claves, encriptaciones, verificaciones, restricciones, niveles de accesos, etc., aun siendo necesarios e imprescindibles, pueden proteger absolutamente los datos computarizados de una persona frente a todos aquellos que, teniendo acceso a los mismos, puedan usarlos para una finalidad incorrecta.

La responsabilidad de todas y cada una de las personas que participan directa o indirectamente en la atención sanitaria de los pacientes y que, por tanto, tienen acceso a sus datos, no podrá ser nunca sustituida por medidas de protección física y técnica de los sistemas de información.

LÍMITES A LA CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

Sin perjuicio de todo lo anterior, tampoco debe olvidarse que los derechos de confidencialidad y de protección de datos, al igual que cualquier otro derecho, no son absolutos. Existen límites y excepciones que se derivan de la colisión con otros derechos o bienes jurídicos dignos de protección y legalmente reconocidos. Se autoriza legalmente el acceso a los datos o su revelación en los siguientes supuestos:

- Cuando se actúa en ***cumplimiento de un deber procesal-penal*** como puede ser ***la obligación de denunciar un delito o el deber de testificar***. La legislación sanitaria recoge un supuesto concreto de levantamiento de la confidencialidad en cumplimiento de los deberes de comunicación y denuncia en el caso de abusos, malos tratos y vejaciones que afecten a niños, personas mayores, mujeres, personas con enfermedades mentales y personas con discapacidad física, psíquica o sensorial.

- Cuando se obra ***para evitar un grave daño en un intento de proteger los derechos y libertades del propio paciente o de terceras personas***. Por ejemplo, si se comunican datos de enfermos mentales cuando estos enfermos pueden ser fuente de daños graves para sí mismos o para otros, y también cuando se da parte de una enfermedad infecciosa a otro miembro de la familia o al centro de trabajo o educativo para evitar el contagio.

- Cuando se comunican ***datos de enfermedades, cuya declaración es obligatoria*** o si es preciso adoptar medidas especiales en materia de salud pública, en cuyo caso el bien que se trata de proteger es la ***salud pública***.

RECOMENDACIONES

1. Dirigidas a los centros sanitarios y a la administración sanitaria:

1.1. ***Desarrollar programas de formación dirigidos a promover entre el personal, tanto sanitario como no sanitario, los valores de la confidencialidad, del cumplimiento del secreto y de una gestión responsable de la información.***

1.2. ***Aplicar y hacer cumplir las medidas de seguridad establecidas por la ley para garantizar la protección de los datos de salud. Esas medidas serán diferentes según se trate de ficheros automatizados o no, pero en cualquier caso han de evitar que se produzcan accesos no autorizados.***

1.3. ***Los responsables de los centros sanitarios deben conocer la efectividad de las medidas de seguridad informática y de control de acceso que se aplican, con el fin de evaluar si hay que modificarlas y/o incrementarlas*.**

1.4. ***Deben establecerse los controles que sean precisos para asegurar que cualquier fichero de datos que se genere a partir de la historia clínica quede registrado, garantizándose que su uso no sea para fines distintos de aquellos para los que fueron recabados.***

1.5. ***Deben quedar registrados todos los accesos a la información, para poder detectar si existe o ha existido un acceso injustificado o irregular, actuando en consecuencia y estableciendo las medidas correctoras oportunas.***

1.6. ***Todos los datos que figuran en la historia clínica tienen el nivel de protección más alto de acuerdo con la Ley de protección de datos de carácter personal; no obstante, es recomendable establecer diferentes niveles de acceso a la información en función del tipo de información a la que se acceda y del perfil profesional de quien accede. En todo caso, deberá tenerse en cuenta si el paciente se ha negado a que dicha información sea compartida.***

2. Dirigidas a los profesionales:

2.1. ***El acceso informático a la información sensible ha de ser personalizado, de tal forma que solo será posible después de identificarse mediante un nombre de usuario y de utilizar una clave de acceso o contraseña.***

2.2. ***La clave de acceso ha de ser personal y secreta, pudiéndose modificar en caso de peligrar su secreto. El personal tiene la obligación de hacer un uso adecuado de su clave y de su preservación.***

2.3. ***Cuando los profesionales, tanto si son sanitarios como si no lo son, conocen legítimamente datos de una persona en el ejercicio de sus funciones, no deben revelarlos sin su consentimiento, ya se trate de datos estrictamente sanitarios o de otros datos personales (domicilio, puesto de trabajo, creencias, opción sexual, estilo de vida, etc.). Esta obligación de secreto persiste incluso cuando finaliza la actividad profesional y sólo puede ceder en aquellos supuestos previstos legalmente.***

2.4. ***Todo aquel que, para el desempeño de sus funciones, llegue a conocer datos confidenciales, debe limitar su acceso a aquello estrictamente necesario, sin olvidar que se encuentra obligado por el deber de secreto***.

2.5. ***Debería diferenciarse entre autorización de lectura de la información y autorización de escritura de información nueva (o modificación de información previa), en cuyo caso deberá quedar registro del cambio producido.***

2.6. ***Como norma no se debería borrar ninguna información, teniendo en tal caso que quedar registro de la modificación introducida y del responsable. No obstante, debe contemplarse la posibilidad de rectificar o cancelar datos a petición del paciente.***

2.7. ***El profesional sanitario solo debe acceder a la información de aquellos pacientes con los que tiene relación asistencial, con autorización para añadir nueva información o escritura (o modificar aquella de la que es responsable). El personal sanitario o no sanitario, no tiene justificación alguna para acceder, ni siquiera para solo lectura, a información sobre pacientes sobre los que no tiene competencia asistencial.***

2.8. ***El profesional sanitario debe ser especialmente cuidadoso cuando transmite información a la hora de solicitar un estudio o una interconsulta, evitando que aparezcan datos especialmente sensibles o datos innecesarios.***

2.9. ***El profesional sanitario tiene el derecho y el deber de poder consultar toda la historia clínica de los pacientes a los que tiene que atender clínicamente, sea cual sea su especialidad médica. La parcela de patología psiquiátrica de la historia clínica también puede y debe ser accesible, al menos en lo concerniente a los diagnósticos, tratamientos y evolución.***

2.10. ***El acceso a la información con fines docentes e investigadores, debe permitirse solo con la autorización expresa del sujeto de investigación y del responsable del servicio asistencial correspondiente, separando los datos de identificación del paciente de los datos de carácter científico-asistencial. Se preservará la identificación directa del paciente mediante un sistema de codificación o anonimización, salvo que éste haya consentido expresamente lo contrario.***

ANEXO 1
NORMATIVA APLICABLE

Constitución Española de 1978.
Art 18.4

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
Art. 197 y Art. 199

Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo del a Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

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

Ley 14/2007, de 3 de julio, de Investigación biomédica.

Real Decreto 223/2004, de 6 de febrero, por el que se regulan los ensayos clínicos con medicamentos

Ley 8/2003, de 8 de abril, sobre derechos y deberes de las personas en relación con la salud.

Decreto 101/2005, de 22 de diciembre, por el que se regula la historia clínica.

Orden HAC/858/2014, de 30 de septiembre, por la que se aprueba la política de seguridad de la información de la Administración de la Comunidad de Castilla y León.

ANEXO 2
BIBLIOGRAFÍA

Beltrán JM., Collazo E., Gervás J., González Salinas P., Gracia D., Júdez J., Rodríguez Sendín JJ., Rubí J., Sánchez M. *Intimidad, confidencialidad y secreto. Guías de ética en la práctica médica.* Ed. Ergón, 2007.
Disponible en:
http://www.fcs.es/docs/publicaciones/guia_final_pdf.pdf

Comisión de Bioética de Castilla y León. *Guía de intimidad, confidencialidad y protección de datos de carácter personal.* 2007.
Disponible en:
http://www.saludcastillayleon.es/profesionales/es/bioetica/guias-bioetica-castilla-leon

Comisión de Bioética de Castilla y León. *Confidencialidad de la información sanitaria: aspectos informáticos.* 2008.
Disponible en:
http://www.saludcastillayleon.es/profesionales/es/bioetica/guias-bioetica-castilla-leon

Igualada Menor A. *Marco legal para usar los datos en salud pública: lo que se puede y lo que se debe hacer*. Actualidad del Derecho Sanitario, nº 159, abril 2009.

Júdez J., Nicolás P., Delgado M. T., Hernando P., Zarco J., Granollers S. *La confidencialidad en la práctica clínica: historia clínica y gestión de la información.*
Med Clin (Barc) 2002;118(1):18-37

Reyero Sánchez, D. *El tratamiento de los datos personales y de salud y la protección de datos*. Diario la Ley, nº 7043, Sección Doctrina, 28 oct.2008, Año XXIX, Ref. D-304, Editorial LA LEY. LA LEY 40117/2008.

Terrón Santos, D. *La regulación de la transmisión de datos médicos a través de redes de telecomunicaciones*. Actualidad Administrativa, nº 9, Sección A Fondo, Quincena del 1 al 15 de MAy.2006, pag.1028, tomo 1, Editorial LA LEY.