

DERECHO DE LOS PACIENTES A LA TRAZABILIDAD DE LOS ACCESOS A SUS DATOS CLÍNICOS

Lola González García

*Grupo de Gestión de la Función Administrativa
Servicio de Salud de Castilla-La Mancha*

SUMARIO: 1.- Introducción. 2.- Datos de carácter personal relacionados con la salud. 3.- Consentimiento para el tratamiento de datos de salud. 4.- Derecho de acceso: 4.1.- Acceso por los profesionales de los centros sanitarios 4.2 -Derecho de acceso del paciente a su historia clínica. 4.3- Derecho de acceso a los registros de accesos. 5. Medidas de Seguridad 6.- Accesos indebidos: Especial referencia a Sentencias condenatorias relevantes. 7.- Conclusiones. 8.- Bibliografía.

RESUMEN

Esta comunicación pretende analizar el derecho fundamental a la protección de datos en el ámbito sanitario desde la perspectiva de la garantía que ofrece este derecho a las personas frente a los posibles accesos indebidos que se producen a la historia clínica. El análisis de este derecho nos obliga a poner en relación dos normas (LOPD y LAP), que debemos estudiar de forma complementaria y no excluyente para dar solución a las numerosas cuestiones que se plantean en relación con la intimidad, confidencialidad, accesos, etc. sobre los datos de salud.

PALABRAS CLAVE

Protección de datos, intimidad, confidencialidad, acceso a la historia clínica, medidas de seguridad, acceso a registros de accesos.

1.- INTRODUCCIÓN

Dentro del ámbito sanitario podemos distinguir dos tipos de derechos fundamentales a la intimidad. Por un lado, el art. 18.1 de la Constitución Española (CE), reconoce el derecho a la intimidad personal que

protege de cualquier invasión que pueda producirse en el ámbito de la vida personal y familiar refiriéndose asimismo a la intimidad corporal. Por otro lado, del art. 18.4 de la citada norma, deriva el derecho fundamental a la protección de datos, que conforme a la doctrina del Tribunal Constitucional¹ se considera como un derecho fundamental independiente y desvinculado del derecho a la intimidad personal y familiar, cuyo objetivo es garantizar a la persona un poder de control sobre sus datos personales. Este poder de control faculta a la persona a decidir sobre qué datos consiente proporcionar a un tercero, permitiéndole además conocer quién posee esos datos y para qué fin, pudiendo oponerse a esa posesión o uso.

Desde la aprobación de 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 (LAP) y posteriormente la normativa en materia sanitaria que complementa este texto, en las Comunidades Autónomas se han regulado determinados aspectos como el acceso

¹ Sentencias del Tribunal Constitucional 254/1993 de 20 de julio, 11/1998, de 13 de enero y 292/2000, de 30 de noviembre

a la documentación clínica, usos profesionales de la historia clínica, acceso de los pacientes (menores, fallecidos, etc).

Esta comunicación pretende analizar el derecho fundamental a la protección de datos en el ámbito sanitario desde la perspectiva de la protección que garantiza este derecho a la personas frente a los posibles accesos indebidos que se producen a la historia clínica. El análisis del mismo nos obliga a poner en relación dos normas que deben estudiarse de forma complementaria y no excluyente para dar solución a las múltiples cuestiones que se plantean en relación con la intimidad, confidencialidad, accesos, etc, sobre los datos de salud. Nos referimos a la Ley Orgánica. 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y su Reglamento de desarrollo, el Real Decreto 1720/2007, de 21 de diciembre y la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica (LAP).

2.- DATOS DE CARÁCTER PERSONAL RELACIONADOS CON LA SALUD

El art. 5.1 g), del Reglamento de la LOPD, define los datos de carácter personal relacionados con la salud como “*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*”. Es decir, el concepto de dato sanitario es realmente amplio y permite incluir información diversa sobre un sujeto determinado². Claro está que las informaciones concernientes a la salud, quedan incorporadas dentro de la historia clínica, que de acuerdo con la LAP, la define como “*el conjunto de documentos relativos a los procesos asistenciales de cada paciente....*”.

DE LA TORRE FORCADELL, define la historia clínica como el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de

un paciente a lo largo del proceso asistencial, no limitándose a ser una mera narración o exposición de hechos, puesto que incluye juicios, documentos, procedimientos, informaciones y sobre todo, el consentimiento del paciente³.

Es decir, la historia clínica es un instrumento que sirve para almacenar y organizar toda la información del paciente relativa a los procesos asistenciales, en ella queda incluida la identificación de los profesionales que le atienden, que serán los que estén legitimados para acceder a ella, obligando a los centros a establecer mecanismos de seguridad que garanticen la intimidad del paciente. Además es una herramienta básica para la investigación biomédica, la educación de estudiantes y la formación médica continua.

Desde la aprobación de la LOPD, se han publicado numerosas normas sobre la historia clínica electrónica⁴. El interés mostrado por el legislador en relación a ésta, destaca la importancia de este soporte, de los datos que contiene y del necesario control, que se debe implantar, del uso y acceso a la información contenida en la misma.

La historia clínica, como instrumento que contiene todos los documentos e informaciones, contiene datos personales relativos a la salud que constituyen un fichero, cuyo tratamiento y uso entra dentro del ámbito de aplicación de la LOPD y su Reglamento de desarrollo y por lo tanto se encuentran protegidos y sometidos a los principios y normas de las mismas.

3.- CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS DE SALUD

En base al principio de vinculación asistencial con el paciente a través de la realización de actos sanitarios por el profesional, se justifica dentro del contexto de la asistencia sanitaria el acceso del profesional sanitario a la documentación clínica del paciente.

Desde la perspectiva de la LOPD, debemos tener en cuenta dos aspectos: por un lado, para tratar los datos personales del paciente, que a su vez lleva implícita la posibilidad de acceder a los mismos, se debe obtener el consentimiento del paciente y por otro lado, antes se debe informar sobre los derechos recogidos en el art. 5.1 de la LOPD.

² Una definición doctrinal, de SERRANO PÉREZ M. M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Thomson- Civitas, Madrid, 2003, pág. 417, quien considera que son toda la información sensible relativa a la salud de un individuo, así como todos aquellos datos personales que es preciso recabar para completar el expediente de esta persona, y que en el campo de la medicina se recoge en lo que se denomina como historia clínica

³ Vid. DE LA TORRE FORCADELL, S., «Reflexiones...», *cit.*, pág. 121.

⁴ La historia clínica surge con la aprobación de la LAP y le siguen todas las Comunidades Autónomas que han regulado los usos y accesos a la misma.

En este punto debemos detenernos y analizar las dos normas conjuntamente, sobre todo para aclarar los artículos 6, 7 y 8 de la LOPD, cuando se refieren a datos de salud.

El art. 6, establece como regla general, que el tratamiento de datos de carácter personal, requiere el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. Igualmente, y para los datos de salud, señala el art. 7.3, que solo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. Sin embargo, el art. 7.6, establece una excepción a lo dispuesto en el 7.3, permitiendo tratar los datos de salud a los profesionales sanitarios sin necesidad de contar con el consentimiento de los mismos, cuando resulte necesario para la prevención, o para el diagnóstico médico, 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 a secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. Además, señala otra excepción, cuando el tratamiento 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. En este último caso subyace el derecho a la vida sobre el derecho a la intimidad o la protección de datos personales⁵. Finalmente, el art. 8 permite a las instituciones y a los centros sanitarios públicos y privados tratar los datos de carácter personal relativos a la 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. Es decir, 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 pues, como afirman SÁNCHEZ CARO J. y ABELLAN F.⁶ *“en la medida en que los actos sanitarios caigan bajo la órbita de la Ley de autonomía del paciente, dicha norma parte del principio del contrato verbal y obliga imperativamente a establecer un contenido mínimo de los datos sanitarios en la historia clínica que necesariamente han de ser tratados”*.

5 STC 53/1985, sin vida no hay derecho a la intimidad.

6 SÁNCHEZ CARO, J. y ABELLÁN, F. *“Datos de salud y datos genéticos. Su protección en la Unión Europea y en España”*, Fundación Salud 2000. Granada, 2004.

Del análisis conjunto de las dos normas objeto de estudio, queda sentado que no es preciso recabar el consentimiento del paciente por parte del profesional sanitario que desea acceder a sus datos de salud, pero siempre por motivos asistenciales y en los supuestos señalados en el art. 7.6. Por lo tanto, para el tratamiento posterior con otra finalidad, sería necesario recabar el consentimiento del paciente, como por ejemplo para la investigación, el reembolso de gastos por un seguro de enfermedad, controlar el absentismo laboral, etc., debido a la interpretación restrictiva que se debe hacer del art. 7.6.⁷

4.- DERECHOS DE ACCESO

Javier Sánchez Caro, al hablar de los principios que asientan la historia clínica electrónica,⁸ señalaba que, para garantizar el derecho a la intimidad y a la confidencialidad, hay que buscar el equilibrio entre la disposición de la información que se almacena en la historia clínica y la protección de datos, regulando de forma restrictiva, pero a su vez pragmática los usos y accesos de los profesionales implicados en la historia clínica.

La LAP, al regular la historia clínica, diferenciaba entre “usos” y “accesos”, utilizando el primer término como sinónimo de finalidad, utilidad u objetivo y el segundo en el sentido de conocer, o de obtener información.

7 Sentencia de la Audiencia Nacional, de 31 de mayo de 2002, mediante la cual aclaró que la excepción del art 7.6 de la LOPD ha de ser interpretada restrictivamente, considerando que es preciso atender en cada caso concreto a que el tratamiento se dirija a la prevención y el diagnóstico.

8 Principios que asientan la HCE, “Son conocidas las ventajas e inconvenientes de la HCE. Entre las primeras destacan la legibilidad, la homogenización y la estructuración, la disponibilidad de acceso, su importante consideración de fuente de información y la seguridad de los datos. A lo que habría que añadir la posibilidad de la aplicación de la telemedicina, la evitación de repetición de pruebas y en general la aplicación de la asistencia sanitaria y la facilidad para la investigación. Pero también sus inconvenientes, siempre mucho menores que sus ventajas, entre los que hay que señalar el esfuerzo adicional que se pide a los profesionales para la introducción de datos, la necesidad de mayores inversiones y recursos y la dependencia que el sistema sanitario contrae con la informatización (dependencia tecnológica). Debe destacarse, además que significa un cambio cultural en el marco de la organización sanitaria y que es obligado extender la citada historia a la totalidad de la población, desde el momento en que aporta beneficios adicionales para los ciudadanos y para los profesionales”.

4.1.- Derecho de acceso por los profesionales de los centros sanitarios

Para hablar del derecho de acceso por los profesionales sanitarios, este mismo autor, se centra en dos principios generales a tener en cuenta para justificar dicho acceso, en orden a su regulación normativa: el principio de vinculación asistencial con el paciente y el principio de proporcionalidad. En relación al primero, señala que la efectiva realización de actos sanitarios por el profesional al paciente es lo que justifica el acceso a la historia clínica y en cuanto al segundo, indica cómo modular el alcance del acceso, basándose en que, la necesidad de proteger la salud de los pacientes obliga a los profesionales a conocer la intimidad de los mismos que consiste en conocer sus datos de salud contenidos en su historia clínica, siempre y cuando ese acceso esté amparado legalmente⁹.

Partiendo de la base de que la información contenida en la historia clínica son datos especialmente protegidos, el acceso indiscriminado al conjunto de datos de salud incorporados a la misma, por parte de los profesionales de los centros sanitarios resulta contrario a lo dispuesto en la LOPD y en la LAP. Por lo tanto, el art. 16 de esta última norma, distingue varios tipos de usos, en función del tipo de profesional y de la necesidad que exista para desarrollar sus propias funciones.

Así pues, permite el acceso a los profesionales asistenciales¹⁰ que realizan el diagnóstico o el tratamiento del paciente, debido a la obligación de estos de cumplimentar la historia clínica, de manera que deberá quedar fechada y firmada la información que se incorpore, de forma que se identifique a la persona que lo realiza.

También permite el acceso a la historia clínica del paciente al personal de administración y gestión, pero este acceso lo limita a los datos relacionados con sus propias funciones. Es decir, la norma distingue entre los profesionales sanitarios que asisten al paciente, del personal de administración y gestión.

Sin embargo, la historia clínica también puede tener otros usos: judiciales, epidemiológicos, de salud pública, de investigación o de docencia. En estos

casos, señala la LAP la obligación de disociar los datos de identificación personal, de los clínico-asistenciales, de manera que quede garantizado el anonimato, salvo que el paciente dé su consentimiento para no disociarlo. La única excepción de permite para no disociar los datos es en los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínicos asistenciales, en cuyo caso se estará a lo que dispongan los jueces y tribunales para ese caso.

Otro colectivo sanitario, al que se permite el acceso a las historias clínicas, son aquellos que ejercen funciones de inspección, evaluación, acreditación y planificación, pero limitado al cumplimiento de sus funciones de comprobación de localización 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.

Sin embargo, con el paso del tiempo y en la práctica diaria, surge la necesidad de consultar información contenida en la historia clínica por otros profesionales que, aunque no son sanitarios, intervienen en la atención al paciente. Nos estamos refiriendo a los trabajadores sociales. Como consecuencia de esta necesidad, algunas normas autonómicas, han decidido regularlo. A modo de ejemplo observamos que la Circular 1/2009 permite el acceso a trabajadores sociales en el mismo sentido que los profesionales de administración y gestión de servicios, solo a los datos estrictamente necesarios para el ejercicio de sus funciones, recordándoles que, en todo caso, quedan sujetos al deber de secreto. Igualmente, en la Comunidad Autónoma de Galicia, el Decreto 164/2013, de 24 de octubre, por el que se modifica el Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica dispone que los trabajadores sociales que desarrollen sus funciones en los centros, servicios o establecimientos sanitarios únicamente podrán registrar su actividad en los apartados correspondientes a aspectos sociales y sociosanitarios de la historia clínica. El acceso mencionado estará restringido a los datos imprescindibles para el ejercicio de sus funciones en relación con su puesto de trabajo, y respetará el derecho a la intimidad personal y familiar de los/as pacientes o usuario/as.

Conviene aclarar qué se consideran profesionales sanitarios que prestan asistencia al paciente. Así la Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias distingue entre *profesiones*

9 SANCHEZ CARO, JAVIER, "La historia clínica electrónica gallega: un paso importante en la gestión del conocimiento" Revista Derecho y Salud, Volumen 18, nº1 enero-junio 2009

10 La Ley 44/2003, de 21 de noviembre, de Ordenación de las profesiones sanitarias (art. 2)

sanitarias tituladas y profesionales del área sanitaria de formación profesional. Considera profesiones sanitarias tituladas y reguladas, aquellas cuya formación pregraduada o especializada se dirige a dotar a los interesados de conocimientos, habilidades y actitudes propias de la atención de salud y que estén organizadas en colegios profesionales oficialmente reconocidos por los poderes públicos, estableciendo dos grupos de nivel: licenciado y diplomado de determinadas titulaciones, dejando la posibilidad de ampliar estas, cuando resulte necesario para mejorar la eficacia de los servicios sanitarios. Asimismo, conforme establece la Ley 10/1986, de 17 de marzo sobre Odontólogos y Otros profesionales, relacionados con la Salud Dental, tienen el carácter de profesional sanitario, la de protésico dental y la de higienista dental. Es decir, el ejercicio de una profesión sanitaria requiere poseer el título oficial que habilite expresamente para ello y se atenderá a lo previsto en la Ley 44/2003, en las demás leyes aplicables y en las normas reguladoras de los colegios profesionales.

En base a ello, los profesionales del área sanitaria de formación profesional, que se estructuran en los grupos de grado superior y grado medio, no se encuentran autorizados para acceder a la historia clínica de los pacientes. Sin embargo, en la práctica diaria, cada vez más, estos profesionales demandan la autorización para acceder a la historia clínica de manera restringida, como en el caso del personal de administración y gestión o de los trabajadores sociales para el ejercicio de sus funciones en relación con su puesto de trabajo, sin embargo hasta ahora, no encontramos ninguna norma jurídica que lo permita.

Es de destacar que hasta este momento, los problemas derivados del acceso, las CCAA los están resolviendo de forma más o menos semejante, pero no debe olvidarse que el acceso a los datos contenidos en la historia clínica de cualquier paciente debe estar regulado en una norma jurídica y además responder a un interés legítimo que sirva de fundamento para dar respuesta a las siguientes preguntas ¿quién puede acceder?, ¿a qué datos?, ¿de qué forma?, ¿para qué? y ser resueltas por las normas legales en función de la casuística.

Una obligación que deben tener presente todos los profesionales que acceden a la historia clínica, es el deber de secreto y la garantía de confidencialidad que se les impone desde diferentes normas¹¹, así

¹¹ Art. 16.6 de la LAP: El personal que accede a los datos de la historia clínica, en el ejercicio de sus funciones queda

como las consecuencias que pueden derivar de su incumplimiento.¹² Estas obligaciones son personales, por lo que será cada uno de los profesionales los que deberán responder individualmente de la vulneración de dichas obligaciones, para ello, insistimos en que la administración sanitaria, debe formar a estos profesionales en temas relacionados con los derechos de los pacientes y concretamente con el derecho fundamental a la intimidad y a la confidencialidad.

4.2 Derecho de acceso del paciente a su historia clínica

El art. 18 de la LAP, reconoce el derecho de acceso al paciente a la documentación de su historia clínica, incluso a obtener copia de los datos que figuran en ella. No obstante, este derecho está sujeto a límites que vienen determinados por el derecho a la confidencialidad que tienen tanto los profesionales que participan en la elaboración de la misma (anotaciones subjetivas), por el derecho de terceras personas que aportan datos al profesional en interés terapéutico del paciente (por ejemplo: un tercero que actúa en beneficio del paciente), así como la

sujeto al deber de secreto.

Art. 10 de la LOPD: El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero, o en su caso, con el responsable del mismo.

Art. 27 del código de deontología médica de julio de 2011: El secreto comporta para el médico la obligación de mantener la reserva y la confidencialidad de todo aquello que el paciente le haya revelado y confiado, lo que haya visto y deducido como consecuencia de su trabajo y tenga relación con la salud y la intimidad del paciente, incluyendo el contenido de la historia clínica. El hecho de ser médico no autoriza a conocer información confidencial de un paciente con el que no se tenga relación profesional

12 STS de 4 de abril de 2001: Se condenó a una médico, que conociendo que la paciente a la que trataba había interrumpido dos veces el embarazo, se lo comunica a una tercera persona y la paciente llega a conocer que la médico ha incumplido el deber de secreto. El Tribunal condena a la autora por delito de revelación de secretos a la pena de un año de prisión y multa de doce meses con cuota diaria de 1.000 pesetas y a la pena de inhabilitación especial para el ejercicio de su profesión por 2 años

TSJ de Extremadura, mediante la cual se condenó a la Administración a abonar una indemnización como consecuencia del ataque a la intimidad del paciente, por revelación de datos personales de la salud de un menor sin el consentimiento expreso de los padres, y sin la finalidad de beneficiar al menor.

Audiencia Provincial de Palma de Mallorca, de 11 de septiembre de 2009, que condenó a un médico de atención primaria a 3 años y tres meses de prisión, multa, e inhabilitación de 9 años por acceder a la historia clínica de un compañero, sin finalidad asistencial, utilizando para ello su clave para el acceso al programa de historia clínica electrónica

información de la que el paciente hubiera sido privado debido a que exista un estado de necesidad terapéutica, debidamente acreditada y siempre que así conste en la historia clínica.

El procedimiento para el ejercicio de acceso se debe ajustar a lo establecido en el Título III del RD 1720/2007. Partiendo de la base de que se trata de un derecho de carácter personalísimo, se ejercerá por el afectado, acreditando su identidad, o por representación voluntaria o legal, debiendo articularse un medio sencillo y gratuito.

El derecho de acceso lo define el art. 27 del RD 1720/2007, como *“el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos”*. Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

4.3 Derecho de acceso a los registros de accesos

Cada vez existe una mayor demanda por parte de los pacientes en conocer la identidad de aquellos que han accedido a su historia clínica, y desde diferentes ámbitos, se viene planteando si el derecho de acceso comprende el derecho a conocer los datos de aquellos profesionales que han accedido a la misma.

El incremento de solicitudes por parte de los pacientes, por sospechar que se están produciendo accesos indebidos a su historia clínica sin fines asistenciales, las variadas sentencias que condenan a profesionales por este tipo de accesos irregulares y la comprobación por parte de los responsables de los ficheros, en el registro de accesos, del aumento de accesos no autorizados que se realizan por los profesionales (ingresos de personajes públicos, en procesos de divorcios, etc.) sin fines asistenciales, hace reflexionar sobre esta cuestión y en la necesidad de regular nuevos mecanismos que garanticen el derecho a la intimidad y a la protección de datos.

Para dar respuesta a esta cuestión nos encontramos con dos posturas completamente distintas.

Inicialmente y antes de la aprobación del Reglamento de desarrollo de la LOPD, la AEPD ya se pronunció en el informe 167/2005, sobre el derecho de acceso señalando que *“el derecho concedido al interesado por la Ley únicamente abarcaría el conocimiento de la información sometida a tratamiento, pero no qué personas, dentro del ámbito de la organización del responsable del fichero han podido tener acceso a dicha información”*. El argumento esgrimido por la AEPD es que la información solicitada en relación a los datos de las personas que han accedido a ese fichero, debe ser considerada como *“datos de carácter personal”*, por lo que su revelación a la interesada, persona distinta del usuario, supondría una *“cesión o comunicación de datos”*, que debería contar con el consentimiento del usuario o encontrarse habilitada por Ley.

Esta misma tendencia sigue el Decreto 24/2011, de 12 de abril, de documentación sanitaria en Castilla – La Mancha, al disponer de forma expresa que el derecho de acceso a la historia clínica no comprende la información sobre los datos personales de las personas que, dentro del ámbito de la organización del responsable del fichero, han podido tener acceso a la misma en el ejercicio de sus funciones.

Por otra parte, y en sentido completamente contrario, nos encontramos con normas autonómicas en el ámbito sanitario, que al regular el derecho a la confidencialidad de la información, como garantía de la misma, reconocen el derecho de las personas a conocer en todo caso quién ha accedido a sus datos sanitarios, el motivo del acceso y el uso que se ha hecho de ellos¹³.

13 Ley Foral 17/2010, de 8 de noviembre, de Derechos y deberes de las personas en materia de salud en Navarra. Art. 31: Toda persona tiene derecho a la confidencialidad de toda la información relacionada con los datos referentes a su salud y estancias en centros sanitarios públicos o privados. Igualmente, tiene derecho a que nadie que no cuente con su autorización pueda acceder a ellos, salvo cuando así lo autorice por razones de interés general la legislación vigente, conforme a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre (RCL 1999, 3058) , de Protección de Datos de Carácter Personal, y 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 del uso codificado de los mismos. Ley 3/2005, de 8 de julio, de Información Sanitaria y Autonomía del Paciente de Extremadura. Art. 35 El derecho de acceso conllevará el derecho del paciente a obtener copias o certificados de los mencionados documentos, y 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 el caso del uso codificado de los mismos, previo pago, en su caso, de las exacciones que se hallen legalmente establecidas

Asimismo, el Dictamen de la Agencia Vasca de Protección de Datos, al analizar la consulta formulada por el Departamento de Sanidad y Consumo del Gobierno Vasco sobre la identificación de personas que han accedido a los datos de un particular en el sistema de identificación de IT de ese departamento, recuerda el alcance del derecho de acceso, mediante un breve resumen de la Sentencia 292/2000, de 30 de noviembre que resulta muy ilustrativo.¹⁴

Continúa el dictamen, dando respuesta a las cuestiones planteadas sobre el número de accesos realizados al registro, y la finalidad de los accesos realizados. La Agencia considera en relación a éstas que, tanto conocer el número de accesos realizados al registro como la finalidad de los accesos realizados forman parte de la información que debe ser ofrecida al solicitante porque constituye en definitiva “...

14 CN11-009, de 17 de mayo de 2011. Breve resumen de la Sentencia TC 292/2000:

“...el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y **que también permite al individuo saber quién posee esos datos personales y para qué**, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, **requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo**, y, por otro lado, el poder oponerse a esas posesiones y usos.

...**resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin**, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, **exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios**.

Por tanto, las facultades legalmente atribuidas a los sujetos concernidos y las consiguientes posibilidades de actuación de éstos son necesarias para el reconocimiento e identidad constitucionales del derecho fundamental a la protección de datos. Asimismo, esas facultades o posibilidades de actuación son absolutamente necesarias para que los intereses jurídicamente protegibles, que constituyen la razón de ser del aludido derecho fundamental, resulten real, concreta y efectivamente protegidos. De manera que, privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo estará también de su derecho fundamental a la protección de datos, puesto que, como concluyó en este punto la STC 11/1981, de 8 de abril (FJ8) “*se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección*”.

información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento, que en su caso se esté realizando...”¹⁵. Conocer estos datos, señala el dictamen, posibilitará al ciudadano saber si sus datos se están utilizando para la finalidad para la que fueron recabados o para otras diferentes, para las que pudiera no existir cobertura legal, con lo que, el ciudadano podría reaccionar interponiendo la correspondiente denuncia ante una autoridad de control.

Resulta clara y garantista la postura adoptada por la Agencia Vasca de Protección de Datos, para la defensa del derecho fundamental a la protección de datos de los pacientes si sospechan de accesos indebidos a su historia clínica, al considerar dentro del derecho de acceso conocer la cantidad de accesos realizados y la finalidad de los mismos. Sin embargo, en cuanto a la pregunta planteada sobre si el derecho de acceso previsto en el art. 15 de la LOPD, incluye el derecho a conocer la identidad de los concretos usuarios que han accedido a sus datos personales, continúa esta Agencia, dando una respuesta negativa y justificándola, conforme a los informes 167/2005, Resolución 558/2007, y Procedimiento de tutela de derechos 1972/2009 de la AEPD.

Aunque los informes de la AEPD y de la AVPD coinciden en interpretar que el derecho de acceso previsto en el art. 15 de la LOPD, no incluye el derecho a conocer la identidad de las personas que han accedido a los datos personales, debemos tener en cuenta que el simple acceso a la historia clínica sin autorización es un delito¹⁶, perseguible solo mediante denuncia de la víctima, salvo que el autor sea un funcionario público. Pues bien, para que el paciente pueda denunciar un acceso indebido, deberá contar con los datos posibles que permitan el derecho de defensa, garantía que se facilita con el derecho reconocido en el art. 35 de la Ley 30/1992, de 26 de noviembre de Régimen Jurídico y Procedimiento Administrativo Común. En este sentido se manifiesta la Sentencia del Tribunal Supremo, de 26 de enero de 2011, al estudiar el art. 35 a) de la citada Ley.¹⁷ En la

15 Art. 27.1 del RD 1720/2007

16 Art. 197 del Código Penal

17 STS, de 26 de enero de 2011 “Para decidir esa cuestión debe comenzar afirmándose que el derecho reconocido en el art. 35º de la 30/1992, está ciertamente dirigido a facilitar el derecho de defensa, y esto lo que significa es ofrecer al interesado la posibilidad de conocer en un procedimiento administrativo todos los hechos y datos que puedan resultar relevantes para la tutela de sus derechos e intereses que quiera ejercitar por cualquier vía (esto es, por la administrativa o por la judicial).

misma dirección se pronuncia el informe de la AEPD 342/2012, “considerando el principio de proporcionalidad y el fin perseguido por la norma (art. 35 a) LRJPAC), se trata de ponderar entre dos derechos fundamentales en juego, el de defensa del art. 24 CE y el de protección de datos de carácter personal del art. 18.4 CE en relación con la STC 292/2000”. Además afirma, como así lo hizo en el informe de 5 de julio de 2010, que “si resultara evidente la necesidad de que el imputado conociera la identidad de los denunciantes para el ejercicio del derecho de defensa habrían de incluirse tales datos identificativos”.

Para finalizar, resulta significativo que el Grupo de trabajo del art. 29, en el Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), adoptado el 15 de febrero de 2007, ya preveía la situación de riesgo que se presentaba con los sistemas de HME. El grupo reparaba en la necesidad de nuevas garantías adicionales en contrapartida, considerando que el mantenimiento de una norma jurídica de confidencialidad resultaba insuficiente para proteger la intimidad de un paciente una vez que los historiales médicos electrónicos se ponen en línea. Asimismo, aclara que los sistemas de HME plantean considerables retos a la hora de garantizar que sólo los profesionales sanitarios habilitados accedan a la información con fines legítimos relacionados con el tratamiento del interesado. A la vista de los riesgos que se presentan, el grupo de trabajo considera necesario prever unos mecanismos de control eficaces para evaluar las garantías existentes. Debido a la complejidad de la información contenida en la HME, junto con la multitud de posibles usuarios, propone nuevos procedimientos por lo que respecta a los derechos de acceso de los interesados. Entre los propuestos se encuentran “introducir un procedimiento especial para informar a los interesados acerca de cuándo y quién ha accedido a su HME, con el fin de tranquilizar a los pacientes al conocer lo que sucede con sus datos en el sistema de HME, así como “realizar controles internos y externos regulares de los protocolos de acceso”, cuya finalidad sea comprobar la legalidad del uso de los datos de los HME. Además señala que la obligación especial de secreto profesional debe ser establecida por normas vinculantes para los profesionales, donde se prevean sanciones efectivas en caso de incumplimiento.

5.- MEDIDAS DE SEGURIDAD

Aunque el nivel de seguridad que se exige para el tratamiento de datos de salud es alto, las sentencias

anteriormente mencionadas demuestran la inquietante preocupación de los pacientes, debido a la inseguridad que produce saber que su intimidad está al descubierto en cualquier momento, puesto que cualquier profesional sanitario (médico/enfermera....) tiene acceso la historia clínica.

Conforme al art. 103 del Reglamento de la LOPD, el responsable del fichero está obligado a adoptar las medidas de seguridad de nivel alto para los ficheros de historia clínica, a elaborar y conservar un registro de accesos. De cada intento de acceso, se guardará como mínimo, la identificación del usuario que accede, la fecha y hora en la que se realizó el acceso, fichero accedido, tipo de acceso y si ha sido autorizado o denegado, debiendo conservar estos datos registrados durante un período mínimo de 2 años. Sin embargo, señala la Resolución de la AEPD, basándose en el criterio adoptado por la Audiencia Nacional, en Sentencias de 13 de junio de 2002 y de 7 de febrero de 2003, que, aunque el Servicio de Salud, disponga de medidas de seguridad que impidan los accesos no autorizados a los datos de carácter personal que contienen las historias clínicas, para el cumplimiento del principio de seguridad de datos, recogido en el art. 9 de la LOPD, razona que “la mera implantación de medidas de seguridad no resultan suficientes, es necesario que se lleven a la práctica”.¹⁸

Pues bien, si el responsable del fichero implanta los niveles de seguridad que establece la normativa de protección de datos, si dispone de un sistema de control de accesos a la historia clínica mediante los cuales se puede detectar los accesos indebidos, nos surgen numerosos interrogantes: ¿Por qué siguen ocurriendo accesos indebidos?, ¿Qué tipo de mecanismos se deben articular para evitarlo?, ¿apertura expediente disciplinario?, ¿comunicación a la autoridad judicial por el responsable del fichero?. Es conveniente, para comprender la importancia de la regulación del uso y acceso a la historia clínica electrónica que desde la propia administración sanitaria se incida en la necesaria preparación intelectual de los profesionales sanitarios sobre el concepto jurídico de confidencialidad de los datos y las consecuencias de la vulneración.

¹⁸ Sentencias de la Audiencia Nacional, en sentencias de 13 de junio de 2002 y de 7 de febrero de 2003 “No basta, entonces, con la adopción de cualquier medida, pues deber ser las necesarias para garantizar aquellos objetivos que marca el precepto. Y, por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva....”.

6.- ACCESOS INDEBIDOS: ESPECIAL REFERENCIA A SENTENCIAS CONDENATORIAS RELEVANTES

Comentado anteriormente el derecho de acceso de los profesionales con fines asistenciales, o para el ejercicio de sus funciones, el problema surge cuando el acceso a la historia clínica de un paciente, se lleva a cabo por un profesional que, pese a tener derecho al mismo, lo realiza con fines distintos a los preestablecidos. Son conocidas por todos las múltiples sentencias que nos encontramos de accesos indebidos por profesionales. Este tipo de acciones se incrementan cuando el paciente es un personaje público (político, actor), en procesos de divorcio, entre compañeros porque existan discrepancias, o porque el caso resulte impactante entre los profesionales. A modo de ejemplo, comentaremos determinadas sentencias que han tenido gran repercusión en el ámbito sanitario, tanto por exigir responsabilidad patrimonial de la Administración por funcionamiento anormal de los servicios públicos o por ser condenatorias para los profesionales con penas de prisión e inhabilitación para la profesión.

En relación a la exigencia de responsabilidad patrimonial de la Administración, traemos a colación, la Sentencia del TSJ de Navarra, de 8 de febrero de 2012. Pues en este caso se demostró el exceso de accesos indebidos (2.825), procedentes de todos los centros del SNS, cuando el paciente en cuestión sólo estuvo en un hospital y en cuatro servicios. Considerando que la Administración no adoptó las medidas de seguridad exigidas para garantizar la protección de datos y del acceso a la historia clínica, al permitir el acceso a personal y profesionales que no tenían que ver con el tratamiento de la paciente.¹⁹

¹⁹ Sentencia TSJ Navarra, de 8 de febrero de 2012. Se trata de una demanda de responsabilidad patrimonial, interpuesta por los familiares de una paciente por haberse producido un funcionamiento anormal del servicio público sanitario, debido a no haber podido impedir el acceso casi indiscriminado de profesionales no implicados en el diagnóstico y tratamiento de la paciente al historial clínico informatizado de la misma. Señala el Tribunal, que queda evidenciado que las medidas de seguridad y protocolo de trabajo de la Administración sanitaria, en orden a garantizar la protección de datos y del acceso a la historia clínica no son suficientes porque no han garantizado esta, al permitir el acceso a personal y profesionales que no tenía que ver con su tratamiento.

Los hechos son concluyentes: 2.825 accesos realizados, por 417 usuarios integrados en 55 servicios y procedentes de todos los centros: hospitales, de salud, ambulatorios etc., del SNS, cuando la paciente solo estuvo en un hospital y en cuatro servicios. Explica el informe pericial que “técnicamente es posible restringir el acceso, y aunque sea difícil delimitar el ámbito de restricción, de alguna manera ha de hacerse pues de otra forma, como el caso demuestra, la ineficacia del sistema

Otra sentencia de especial relevancia fue la de la SAP de Palma de Mallorca, de 11 de febrero de 2009, que condenó a un médico de atención primaria a 3 años y tres meses de prisión, multa e inhabilitación de 9 años por acceder a la historia clínica de un compañero, sin finalidad asistencial, utilizando para ello su clave para el acceso al programa de historia clínica electrónica. Esta fue recurrida y mediante STS 1328/2009, de 30 de diciembre, se absuelve al Coordinador de un delito continuado de acceso a datos reservados de carácter personal, por entender que averiguar el nombre del médico de cabecera, no era “descubrir” un secreto, al no tratarse de un dato privado, sino público, al que podía tener acceso cualquier persona, a través de la cita previa, además de demostrarse que el acceso sin autorización no causó perjuicio al titular del dato.²⁰

Tal y como hemos comentado anteriormente, incluso en procesos de divorcio resulta frecuente acceder a la historia clínica del cónyuge, o como se trata en este caso de la pareja del cónyuge, para utilizar algún dato de salud de la misma. En este caso, se trata de una enfermera que durante el proceso de divorcio de su hermana, accede con su clave a la historia clínica de la pareja de su ex cuñado, con la finalidad de comprobar si padecía algún trastorno psiquiátrico y facilitarle esa información a su hermana que a su vez se la comunicaría a su letrada. Esta presentó en el juzgado la solicitud de una suspensión cautelar del régimen de visitas que disfrutaba el padre de los hijos

arbitrado es absoluta. Concluyendo que el acceso se ha de facilitar a los profesionales que atienden al paciente y no a todos”

²⁰ Una de las cuestiones que se plantean es si el profesional en su condición de coordinador del centro de salud, puede acceder al dato del médico de cabecera del denunciante. El TS considera que “una cosa es que el recurrente en su condición de coordinador pudiera estar autorizado a conocer el nombre del médico de cabecera, en el cumplimiento de las funciones a que se refiere el art. 16.5 de la LAP y otra muy distinta es que, sin expediente incoado, ni denuncia alguna, acceda a este dato de la forma en que lo hizo: introduciendo en la agenda de sus pacientes el nombre del denunciante, que no era paciente suyo, esto es, con una utilización incorrecta del programa informático del que disponía”.

Otra de las cuestiones planteadas, era dar respuesta a si el dato de identidad del médico de cabecera, compañero del centro de salud, se considera dato protegido penalmente, esgrimiendo para dar respuesta, los siguientes motivos:

- No es un dato personal reservado o secreto, porque cualquier persona podría acceder a este tipo de datos no sanitarios a través de cita previa o acudiendo al servicio de tarjeta sanitaria de la Gerencia.
- El hecho de que el dato no tenga la consideración de “sensible”, no supone que haya de descartarse la posibilidad de lesividad que puede entrañar el acceso sin autorización a tales datos. Es decir, debería acreditarse el perjuicio causado al titular del dato, que en este caso no se ocasionó.

de ambos. El acceso a esos datos, lo justifica la enfermera en ayudar a su hermana y proteger a los hijos de ésta. Sin embargo, el TS considera que los móviles a estos efectos, son irrelevantes, señalando que, el hecho de que actuara con la finalidad de ayudar a los menores, no justifica su conducta y la vulneración del derecho fundamental a la intimidad se encuentra delimitado en el art. 197 del Código Penal²¹.

El art. 197 tipifica como delito, el acceso a la historia clínica por quien no esté legitimado para ello. Además, se trata de un delito que solo es perseguible mediante una denuncia de la víctima, salvo que el autor sea un funcionario público. Es decir, si el paciente no tiene conocimiento de la identidad de quién ha accedido indebidamente para poder denunciarlos, éstos quedarán impunes. Solo en el caso de que sean funcionarios públicos, podrían iniciarse acciones legales contra ellos, si el responsable del fichero conociera los hechos y los denunciara ante la autoridad judicial.

Reflexiona Sergio Gallego Riestra²², sobre la necesidad de adoptar medidas, tanto éticas como jurídicas para evitar los accesos indebidos a la historia clínica, justificándolo en las múltiples sentencias que demuestran este tipo de accesos y la indefensión que toleran los pacientes a la hora de demostrar que se han realizado accesos indebidos, pues se les deniega el derecho a conocer la identidad de las personas que han accedido a ella, haciendo una interpretación restrictiva del derecho de acceso reconocido en la LOPD y en la LAP. Subraya el autor que, solo como una prueba pedida a través de un juez dentro de una causa criminal, se podría obtener el listado de accesos que las organizaciones sanitarias niegan frecuentemente al solicitarlo el paciente.

7.- CONCLUSIONES

Está claro que el derecho fundamental a la protección de datos, garantiza a la persona un poder de control sobre sus datos personales. Este poder de control faculta a la persona a decidir qué datos proporciona a un tercero o cuales de ellos le permite recabar. Además le permite saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso. Sin embargo, una interpretación restrictiva del derecho de acceso regulado en el art. 15 de la LOPD,

realizada por la AEPD o por los Gestores de los centros sanitarios, señala que éste, no comprende el derecho a conocer la identidad de las personas que han accedido a la misma.

Del estudio conjunto de las dos normas objeto de estudio de esta comunicación, se puede afirmar que en virtud del principio de vinculación asistencial no es preciso recabar el consentimiento del paciente por parte del profesional sanitario que desea acceder a sus datos de salud, pero siempre por motivos asistenciales y en los supuestos señalados en el art. 7.6. No obstante, las normas jurídicas son las que permiten qué profesionales pueden acceder a la historia clínica y el tipo de acceso que pueden realizar, siempre dependiendo de las necesidades existentes para el desarrollo de sus funciones. Asimismo, el Código Penal considera delito el acceso a la historia clínica sin autorización.

Para reforzar esta garantía, los responsables de los ficheros están obligados a adoptar las medidas de seguridad que permitan asegurar el derecho a la protección de datos, quedando registrados la identidad de las personas que acceden, la fecha y hora, parte de la historia a la que se accede, y tipo de acceso, incluso de los accesos denegados. Por lo que poseemos mecanismos para detectar este tipo de accesos y por lo tanto disminuir el uso de esta práctica tan habitual en cualquier parte del territorio del SNS.

Por todo ello, debemos pararnos y reflexionar: Si normativamente, se encuentra regulado todo el contenido de este derecho: el nivel de protección alto para datos de salud, la creación de un registro que deje huella, los profesionales que se les permite acceder, ¿Qué falla?. Si en la mayoría de los casos los accesos se producen por profesionales que por su perfil profesional tienen acceso, pero lo hacen sin fines asistenciales. ¿Qué se consigue con hacer una interpretación restrictiva del derecho de acceso recogido en la LOPD?, ¿acudir con mayor frecuencia a los tribunales?

Pues bien, desde nuestro punto de vista, para resolver este conflicto y garantizar del derecho a la protección de datos de los interesados dentro del ámbito sanitario, se proponen dos acciones:

- La primera, como apunta MILLÁN CALENTI “desde la propia Administración sanitaria resulta necesario que se incida en la preparación intelectual de los profesionales sanitarios sobre el concepto jurídico de confidencialidad de los

21 STS, de 18 de octubre de 2012

22 GALLEGO RIESTRA, SERGIO “¿Tiene el paciente derecho a saber quiénes y por qué han accedido a su historia clínica?, Volumen 22, nº1 Enero-junio 2012

datos y las consecuencias de la vulneración”²³. A esta medida, yo añadiría otra que está en manos de la Administración. La investigación de los posibles accesos indebidos, cuando un paciente sospeche de ello y el establecimiento de mecanismos necesarios que sirvan para disuadir a los profesionales de este tipo de prácticas.

- La segunda, la señala GALLEGO RUESTRA, postura que también comparto²⁴. El considera que la única forma de garantizar que el paciente pueda ejercer las acciones pertinentes para proteger su derecho a que no se produzcan intromisiones ilegítimas a su historia clínica, es “*reconociendo el derecho de acceso al registro de los accesos producidos, y pudiendo solicitar cuanta información estimen conveniente sobre la legitimidad de los mismos*”. El no ve inconveniente en “*entender que los accesos son equiparables a las cesiones, o bien considerando este derecho independiente y desligado del derecho de acceso a los ficheros informáticos, pero en ambos casos, proporcionando los listados de usuarios a fin de garantizar realmente la protección a la intimidad*”.

8. BIBLIOGRAFIA

- SANCHEZ CARO, JAVIER, “La historia clínica electrónica gallega: un paso importante en la gestión del conocimiento” Revista Derecho y Salud, Volumen 18, nº1, 2009
- SÁIZ RAMOS, MACARENA y LARIOS RISCO DAVID. “El derecho de acceso a la historia clínica por el paciente: propuesta para la reserva de anotaciones subjetivas”. Revista Derecho y Salud. Volumen 18, nº1, 2009
- BELTRÁN AGUIRRE, JUAN LUIS. Tratamiento de datos de salud en la prestación de servicios sociales. Revista Derecho y Salud. Volumen 18, nº1, 2009

- BELTRÁN AGUIRRE, JUAN LUIS, “La protección de los datos personales relacionados con la salud”. <http://www.navarra.es/NR/rdonlyres/517A4434-9C3B-442E-8651-61A7AE0490AD/226320/pdps.pdf>

- SERRANO PÉREZ, M^a MERCEDES Salud Pública, epidemiología y protección de datos. En Tratado de Derecho Sanitario. Directores: Alberto Palomar Olmeda y Josefa Cantero Martínez

- GARCÍA AMEZ, JAVIER La protección de datos del usuario de la sanidad: derecho a la intimidad y asistencia sanitaria.

- SERRANO PÉREZ, M^a MERCEDES, La protección de los datos sanitarios. La historia clínica. https://www.uclm.es/actividades0506/seminarios/proteccion_datos/pdf/datos_sanitarios.pdf

- SERRANO PÉREZ M. M., El derecho fundamental a la protección de datos. Derecho español y comparado, Thomson- Civitas, Madrid, 2003

- GALLEGO RUESTRA, SERGIO “¿Tiene el paciente derecho a saber quiénes y porqué han accedido a su historia clínica?”, Volumen 22, nº1 Enero-junio 2012

- GALLEGO RUESTRA, SERGIO. “Historia clínica electrónica y derecho a la autonomía del paciente: un conflicto de intereses”. Disertación de ingreso como Académico Correspondiente en la Real Academia de Jurisprudencia del Principado de Asturias, el día 22 de noviembre de 2013

- MILLÁN CALENTI, RAFAEL. Historia clínica electrónica: accesos compatibles. En Tratado de Derecho Sanitario. Directores: Alberto Palomar Olmeda y Josefa Cantero Martínez

- HEREDERO HIGUERAS, M., La Directiva Comunitaria de Protección de los Datos de Carácter Personal, Aranzadi, Elcano, 1997

- APARICIO SALOM, J., Estudios sobre la Ley Orgánica de Protección de Datos de Carácter Personal, 2a ed. Cizur Menor (Navarra): Aranzadi, 2002

- LARIOS RISCO, DAVID. Protección de datos personales y administración electrónica. Administración electrónica: sede, gobierno y contratación. Coord. Rafael Alvaro Millán Calenti; Fernando Suárez Lorenzo (dir.), 2012,

23 MILLÁN CALENTI, RAFAEL. Historia clínica electrónica: accesos compatibles en “Tratado de derecho sanitario”, Coordinador.....

24 GALLEGO RUESTRA, SERGIO “¿Tiene el paciente derecho a saber quiénes y porqué han accedido a su historia clínica?”, Volumen 22, nº1 Enero-junio 2012

- LARIOS RISCO, DAVID “La historia clínica como conjunto de datos especialmente protegidos”. El derecho a la protección de datos en la historia clínica y la receta electrónica, 2009,
- GÓMEZ PIQUERAS, CRISTINA, “La historia clínica. Aspectos conflictivos resueltos por la Agencia Española de Protección de Datos”. El derecho a la protección de datos en la historia clínica y la receta electrónica, 2009