CEBES
CENTRO DE ESTUDIOS EN BIODERECHO, ÉTICA Y SALUD
UNIVERSIDAD DE MURCIA

INTIMIDAD, CONFIDENCIALIDAD Y PROTECCIÓN DE LA INFORMACIÓN SANITARIA. ESTUDIO PRÁCTICO DEL ACCESO AL APLICATIVO SELENE POR FACULTATIVOS DEL SERVICIO MURCIANO DE SALUD.

PABLO VIGUERAS PAREDES

Jefe de Servicio de Asesoría Jurídica
Hospital Clínico Universitario "Virgen de la Arrixaca"
Profesor Asociado de Derecho Civil
Universidad de Murcia

pablo.vigueras@gmail.com

MARÍA ENCARNACIÓN HERNÁNDEZ CONTRERAS

Servicio de Medicina Interna
Hospital Clínico Universitario "Virgen de la Arrixaca"
Profesora Asociada de la Universidad de Murcia

maencarna79@gmail.com

RESUMEN: En el presente trabajo se ha intentado conjugar desde el punto de vista práctico cuestiones como la intimidad y confidencialidad y práctica clínica. Ambas cuestiones adquieren un especial carácter cuando se trata de datos clínicos. El especial cuidado que deben llevar los profesionales sanitarios debe conjugarse con los avances de las herramientas informáticas. Frente a la mayor accesibilidad del profesional se incrementan los peligros del acceso indebido. Las medidas de seguridad que deben implantarse deben ser inversamente proporcionales a la facilidad en el acceso.

PALABRAS CLAVE: Medicina, intimidad, protección de datos.

ABSTRACT: In the present work we have tried to combine from the practical point of view issues such as intimacy and confidentiality and clinical practice. Both issues acquire a special character when it comes to clinical data. The special care that health professionals must take must be combined with the advances of computer tools. Faced with the greater accessibility of the professional, the dangers of undue access increase. The security measures that must be implemented must be inversely proportional to the ease of access.

KEYWORDS: Medicine, intimacy, data protect.

I. INTRODUCCIÓN

La información sanitaria obtenida en la relación médico-paciente esta sujeta a la mas estricta confidencialidad, pues deriva de la confianza del paciente depositada en el profesional sanitario y somete a éste al deber de secreto, so pena de ser reprobado no solamente desde el punto de vista moral o administrativo, sino incluso penal.

Hipócrates (siglo V antes C.) redactó el famoso juramento[1], posteriormente consagrado por Galeno, en el que ya recogía la obligación de guardar silencio sobre la información obtenida del paciente en el ejercicio de la Medicina. Dicho principio, modernizado, se identifica como fundamento del ya citado secreto médico, y se ha mantenido en la actualidad con algunas excepciones legales, como las enfermedades de declaración obligatoria o los supuestos de comisión de delito.

Las obligaciones de custodia y conservación de la información clínica están suficientemente explicitadas en los artículos 14.4, 16.6 y 17 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, que hace responsable a las Comunidades Autónomas de aprobar todas las disposiciones necesarias para que los centros sanitarios adopten las medidas técnicas (reguladas en legislación de protección de datos de carácter personal) y organizativas para archivar y proteger las historias clínicas; que somete al secreto profesional (y, por tanto a las consecuencias de su vulneración) al que en el ejercicio de sus funciones acceda a una historia clínica.

La implantación de las llamadas Tecnologías de la Información y la Comunicación (TIC) ha revolucionado la actividad sanitaria. Supone en esencia, que la información sanitaria ha dejado de constituir un soporte físico (la historia clínica y el archivo tradicional de historias clínicas) para convertirse en un soporte informático integrado con la información contenida en servidores, no necesariamente en la institución de la que procede la información, y que han dado lugar a lo que se conoce como historia clínica electrónica.

Es rigurosamente cierto que las posibilidades de explotación de la citada información, así como la disponibilidad inmediata y la rapidez en el acceso son ventajas indudables de estas tecnologías, y ello debiera repercutir en la mejora de la calidad de la asistencia sanitaria. Pero no es menos cierto que existen riesgos indudables, entre los que destaca sobremanera el acceso indebido a los datos e información sanitaria.

En el presente trabajo hemos intentado plasmar también, tras una introducción teórica, las conclusiones generales de la realización de un estudio práctico llevado a cabo en 2016 y 2017 sobre el acceso al aplicativo de historia clínica institucional del Servicio Murciano de Salud (SELENE) por parte de los facultativos del Hospital Clínico Universitario "Virgen de la Arrixaca", con el ánimo de introducir medidas de concienciación del personal, y mejorar la salvaguarda de la intimidad del paciente.

[1] "Guardaré silencio sobre todo aquello que en mi profesión, o fuera de ella, oiga o vea en la vida de los hombres que no tenga que ser público, manteniendo estas cosas de manera que no se pueda hablar". (http://www.bioeticanet.info/documentos/JURHIP.pdf)

II. CONSIDERACIONES GENERALES SOBRE LA INTIMIDAD, CONFIDENCIALIDAD Y LA PROTECCIÓN DE DATOS SANITARIOS

Se ha escrito mucho sobre la cuestión de la confidencialidad e intimidad tanto a nivel general como de forma específica en el ámbito sanitario. No pretendemos aquí extendernos en abordar la problemática de estas cuestiones tan interesantes, sino meramente fijar una posición inicial que nos centre en la cuestión.

CORBELLA I DUCH[2] ha resaltado que la prestación sanitaria no se puede realizar sin conocer datos, hechos y actuaciones de la persona y sin explorar partes de su cuerpo que no se expone a la vista de los demás, por cuyo motivo el paciente debe abrir la puerta de la esfera de la intimidad, y en ocasiones, hasta el ámbito más reducido de sus secretos, para hacer posible la actuación sanitaria.

La Constitución Española[3], en su artículo 18.4 dispone que la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. De ambos preceptos deriva el derecho fundamental a la protección de datos de carácter personal, que ha sido definido como autónomo e independiente por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre[4].

BELTRÁN AGUIRRE[5] indica que, según señala la STC 2000/292, de 30 de noviembre[182], ambos derechos comparten el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar. Pero la peculiaridad del derecho fundamental a la protección de datos radica en su distinta función, objetivo y contenido. La función del derecho fundamental a la intimidad (artículo 18.1 CE) es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar. En cambio, el derecho fundamental a la protección de datos (artículo 18.4 CE) persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir un tráfico ilícito y lesivo para su dignidad. Así, el objeto del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino la reserva de todos los datos de carácter personal, particularmente los informatizados.

LARIOS RISCO Y SÁIZ RAMOS[6] mantienen que el derecho de los ciudadanos a controlar sus datos personales forma parte del contenido esencial del derecho a la intimidad personal y familiar reconocido en el artículo 18.1 de la Constitución; pero sobre todo es un instrumento para garantizar la eficacia del derecho fundamental a la protección de datos (artículo 18.4 de la Constitución). Ciertamente se trata de derechos diferentes. Así, en tanto que la función del primero es proteger a la persona frente a cualquier invasión que pueda realizarse en aquel ámbito de su vida que el individuo desea excluir del conocimiento ajeno y de las

[2] CORBELLA J. Manual de Derecho Sanitario. 2ª ed. Barcelona: Atelier Libros S.A, 2ª ed., 2012.

[3] Constitución Española de 27 de diciembre de 1978. Boletín Oficial del Estado, núm. 311, p. 29313, (29 de diciembre de 1978).

[4] Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Tribunal Constitucional. Sentencia 292/2000, de 30 de noviembre de 2000. Boletín Oficial de Estado, nº 4 (suplemento), p. 104. (4 de enero de 2001)

[5] BELTRÁN JL. Tratamiento de datos de salud en la prestación de servicios sociales. Derecho y Salud. 2009; 18 (1):1-19.

[6] LARIOS D, SÁIZ M. El derecho de acceso a la historia clínica por el paciente: propuesta para la reserva de anotaciones subjetivas. Derecho y Salud. 2009 18 (1):21-41.

intromisiones de terceros en contra de su voluntad, el segundo otorga a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir un tráfico ilícito y lesivo para la dignidad del afectado.

También BELTRÁN AGUIRRE[7] ha resaltado que la función del derecho fundamental a la intimidad (artículo 18.1 CE[69]) es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar. Protege la intimidad personal, de la que forma parte la intimidad corporal (STC 37/1989), que en nuestro ámbito se traduce, por ejemplo, en poder disponer de habitación individual, y la llamada intimidad territorial, que significa que no se conozca o se haga pública la estancia de una persona en un centro sanitario. En cambio, el derecho fundamental a la protección de datos (artículo 18.4 CE[69]) persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir un tráfico ilícito y lesivo para su dignidad.

Esa protección de la intimidad tiene su traducción en la normativa española desde diversas perspectivas. Así, el Derecho Penal regula el tipo delictivo de descubrimiento y revelación de secretos (artículos 197 a 201[8] y 463 ó 556 de la *Ley Orgánica 10/1995, del Código Penal*[9]). El Derecho Civil protege la intimidad principalmente a través de la *Ley Orgánica 1/1982*[10]*, de 5 de mayo, de Protección Civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*, considerando intromisión ilegítima (artículo 7) la "divulgación de hechos relativos a la vida privada de una persona o familia que afecte a su reputación y buen nombre" y la "revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela"[11]. Desde el punto de vista laboral, existen innumerables preceptos destinados a la protección de la intimidad de los trabajadores. Así, por ejemplo, el *Real Decreto Legislativo 1/1995, de 24 de marzo, Texto*

[7] BELTRÁN JL. La protección de datos personales relacionados con la salud. Ponencia del Defensor del Pueblo de Navarra, (27 de junio de 2012).

[8] Especialmente interesante es el art. 199.2 del Código Penal de 1995 que se refiere al "profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años". La Sentencia del Tribunal Supremo 574/2001, de 4 de abril condena a un facultativo por la comisión de un delito de divulgación de secreto del art. 199.2, a un año de prisión y multa de doce meses, y a la inhabilitación especial para el ejercicio de su profesión por dos años, así como a una indemnización a la perjudicada de dos millones de pesetas. Los hechos se refieren a los comentarios realizados por la profesional a su madre sobre datos contenidos en la historia clínica de una paciente conocida previamente por ambas, relativos a dos procesos quirúrgicos previos de interrupción legal de embarazo, y a su posterior difusión por la madre, llegando a conocimiento de la hermana de la citada paciente. En la sentencia se indica que "La acción típica consiste en divulgar los secretos de una persona entendida como la acción de comunicar por cualquier medio, sin que se requiera que se realice a una pluralidad de personas, toda vez que la lesión del bien jurídico intimidad se produce con independencia del número de personas que tenga conocimiento"; y añade que "Por secreto ha de entenderse lo concerniente a la esfera de la intimidad, que es sólo conocido por su titular o por quien él determine. Para diferenciar la conducta típica de la mera indiscreción es necesario que lo comunicado afecte a la esfera de la intimidad que el titular quiere defender".

[9] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado, núm. 281, p. 33987, (24 de noviembre de 1995).

[10] Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al honor, a la intimidad personal y familiar y a la propia imagen. Boletín Oficial del Estado, nº 115, p. 12546, (14 de mayo de 1982).

[11] La Sentencia del Tribunal Supremo de 18 de octubre de 2004 señala que "Esta Sala tiene declarado que la aparente incompatibilidad entre el Art. 18.1 y el Art. 20 CE, ha de resolverse a favor del segundo cuando la noticia publicada sea de interés general, afecte al orden social o al conjunto de los ciudadanos y esté revestida de veracidad; y, asimismo, que la reproducción por la fotografía de la imagen de una persona en su vida privada o fuera de ella, no constituye intromisión ilegítima cuando la publicación se refiere a personas que ejerzan una profesión de notoriedad o proyección pública, y la imagen, se capte durante un acto público o en lugares abiertos al público, cuando la imagen de una persona aparezca como accesoria. Pero, nada de esto ocurre en el supuesto de autos, debiendo tener en cuenta, además, que las imágenes de las menores, están especialmente protegidas en nuestro ordenamiento jurídico".

Refundido del Estatuto de los Trabajadores[12] (Artículos 4.2 y 18), la *Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical*[13] (artículo 10.3.1º), la *Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales*[14] (artículo 22.4) o el *Real Decreto 39/1997, de 17 de enero, Reglamento de los Servicios de Prevención*[15] (artículo 37.3.d). Desde el punto de vista administrativo destaca la normativa de protección de datos, constituida por la Ley Orgánica de Protección de Datos[16] de 1999 y su reglamento de 2007, al que haremos referencia más adelante. Finalmente, también desde el punto de vista deontológico, destaca el Código de Deontología Médica de 2011 (artículo 9)[17].

Recientemente, la Unión Europea ha intensificado las medidas protectoras a través de un nuevo reglamento europeo de protección de datos[18], debido, entre otras razones, a una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en particular en relación con las actividades en línea.

La finalidad última de la Legislación de Protección de Datos puede sintetizarse en dos objetivos: el primero, garantizar al interesado determinados derechos y principios (acceso, rectificación, oposición y cancelación; información, calidad de los datos exigiendo que éstos sean adecuados, pertinentes y no excesivos); el segundo, adoptar medidas de seguridad adecuadas al tipo de datos y además todas aquéllas que la lógica y la prudencia exijan para "evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos" (artículo 9 Ley Orgánica de Protección de Datos).

Aplicado a datos sanitarios, la primera referencia postconstitucional del derecho a la intimidad y confidencialidad se encuentra en la Ley General de Sanidad de 1986[19], cuyos artículos 10.1 y 10.3 reconocen respectivamente que el paciente tiene el derecho "Al respeto a su personalidad, dignidad humana e intimidad, sin que pueda ser discriminado…" y el derecho "A la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público".

Como ha destacado TRONCOSO REIGADA[20], la gestión de la asistencia y de los servicios sanitarios en atención primaria, en atención especializada y en la urgencia exige necesariamente una acumulación masiva de información personal de los ciudadanos pues es a éstos a los que se les trata de garantizar su salud. Además de la asistencia sanitaria como derecho subjetivo, la salud pública es un bien jurídico colectivo. Existe un interés social que

[12] Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. Boletín Oficial del Estado, nº 75, p. 9654, (29 de marzo de 1995).

[13] Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical. Boletín Oficial del Estado, nº 189, p. 16660, (8 de agosto de 1985).

[14] Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales. Boletín Oficial del Estado, nº 269, p. 32590, (10 de noviembre de 1995).

[15] Real Decreto 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención. Boletín Oficial del Estado, nº 27, p. 3031, (31 de enero de 1997).

[16] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado nº 298, p. 43088, (14 de diciembre de 1999).

[17] Código de Deontología Médica. Colegio Oficial de Médicos de España. Julio de 2011.

[18] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE de 4 de mayo de 2016).

[19] Ley 14/1986, de 25 de abril, General de Sanidad. Boletín Oficial del Estado, nº 102, p. 15207, (29 de abril de 1986).

[20] TRONCOSO A. La protección de datos personales. En busca del equilibrio. 1ª ed. Valencia: Tirant Lo Blanch, 2010.

comprende los beneficios colectivos de la investigación médica y las políticas de prevención y de salud pública, actividades éstas que se materializan sobre información sanitaria de personas.

Ahora bien, ¿Qué entendemos por datos sanitarios? La AEPD, en informe jurídico 129/2005[21] nos recuerda que "El apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa viene a definir la noción de "datos de carácter personal relativos a la salud", considerando que su concepto abarca "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo", pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. Añade el citado apartado 45 que "debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas". En este mismo sentido, la Recomendación nº R (97) 5, del Comité de Ministros del Consejo de Europa, referente a la protección de datos médicos afirma que "la expresión datos médicos hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas. El apartado 38 de la mencionada Recomendación considera igualmente, siguiendo lo señalado en el Convenio 108 que la expresión "datos médicos debería incluir igualmente cualquier información que ofrezca una visión real sobre la situación médica del individuo", incluyendo datos como los referidos al "abuso de las drogas, abuso de alcohol y nicotina o consumo de drogas".

También la AEPD, en el informe jurídico 471/2008[22], también resalta que "La especial protección conferida a los datos relacionados con la salud de las personas no es arbitraria, sino que resulta de lo dispuesto en las normas Internacionales y Comunitarias reguladoras del tratamiento automatizado de datos de carácter personal. En este contexto, tanto el artículo 8 de la Directiva 95/46/CE del Parlamento y del Consejo, así como el artículo 6 del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, ratificado por España en fecha 27 de enero de 1984, hacen referencia a los datos de salud como sujetos a un régimen especial de protección".

A falta de desarrollo legislativo, hubo que esperar a que la *Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*[23] abordara una primera protección de los datos personales y, específicamente, en los artículos 7 y 8, los datos de salud como especialmente protegidos. Concretamente, en el artículo 7.3 se decía que: "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente".

Y el artículo 8 continuaba: "Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento automatizado de 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 los artículos 8, 10, 23 y 61 de la Ley 14/1986, de 25 de abril, General de Sanidad; 85.5, 96 y 98 de la Ley 25/1990, de 20 de diciembre, del Medicamento[24];

[21] Informe jurídico 129/2005. Agencia Española de Protección de Datos. 2005.

[22] Informe jurídico 471/2008. Agencia Española de Protección de Datos. 2008.

[23] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Boletín Oficial del Estado, nº262, p. 37037, (31 de octubre de 1992).

[24] Ley 25/1990, de 20 de diciembre, del Medicamento. Boletín Oficial del Estado, nº 306, p. 38228, (22 de diciembre de 1990).

artículos 2, 3 y 4 de la Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública[25], y demás Leyes sanitarias".

Es decir, ya consideraba como datos especialmente protegidos a los datos de salud, requiriendo, para ser recabados, ser tratados y cedidos el consentimiento del afectado.

La Ley Orgánica de Protección de Datos de 1999 y su desarrollo por Real Decreto 1720/2007[26], junto con la Ley de Autonomía del Paciente de 2002 en el ámbito sanitario, constituyen las normas principales, aplicables en España. Dichas Leyes deberán necesariamente adaptarse a las medidas mas proteccionistas impuestas por el nuevo Reglamento europeo de 2016 que en este campo aluden especialmente a la investigación científica, a los datos genéticos y a la extensión del concepto relativo a los datos de salud.

La redacción de la Ley Orgánica 15/1999 suprime la referencia al tratamiento automatizado de los datos, incluyendo por tanto cualquier tipo de tratamiento, sea o no automatizado. En lo demás, no varía sustancialmente la redacción de la anterior legislación. Señala, pues, la Ley Orgánica de Protección de Datos, en su artículo 7.3. que "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".

A continuación, añade, en el apartado 6, con mayor rigor que la redacción de 1992: "No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento 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 al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior 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".

Es decir, establece distintas excepciones a la exigencia de la prestación del consentimiento, como son la prevención o el diagnóstico médico, la necesidad de tratar los datos para la propia prestación del servicio sanitario, y los supuestos de urgencia vital, incluida la incapacitación del afectado para prestar el consentimiento.

Igualmente, queda aclarado en el artículo 8 la autorización legal para el tratamiento de los datos de salud cuando señala: "Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de 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".

Por su parte, el Reglamento de 2007 somete en su artículo 81.3 a) a los datos de salud a las medidas de seguridad de nivel alto (artículos 111-114).

[25] Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales de salud Pública. Boletín Oficial del Estado, nº 102, p. 15207, (29 de abril de 1986).

[26] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Boletín Oficial del Estado, nº 17, p. 4103, (19 de enero de 2008).

La Ley de Autonomía del Paciente, en su Exposición de Motivos[27], justifica suficientemente la relevancia y necesidad de la protección. El contenido de la Ley resulta acorde con ello, al figurar dentro de los principios básicos del artículo 2 que: "1. 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". … "7. La persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida".

El Capítulo III (artículo 7) está dedicado a la intimidad configurándola como derecho de los pacientes y obligación de los centros sanitarios: "1. 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. 2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes".

Parece pues, que si ya resulta clara, por sí misma, la cuestión de la necesidad de protección general de los datos de salud, adquiere especial importancia el respeto a la intimidad al abordar la historia y documentación clínica. Así en el artículo 16.3 de la Ley de Autonomía del Paciente se dice que: "El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso".

El artículo 16.6, por su parte, añade que "el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto". Y el artículo 17.6 hace referencia a las denominadas medidas de seguridad cuando especifica que "son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica de Protección de datos de Carácter Personal".

[27] Indica la Exposición de Motivos que "La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, califica a los datos relativos a la salud de los ciudadanos como datos especialmente protegidos, estableciendo un régimen singularmente riguroso para su obtención, custodia y eventual cesión. Esta defensa de la confidencialidad había sido ya defendida por la Directiva comunitaria 95/46, de 24 de octubre, en la que, además de reafirmarse la defensa de los derechos y libertades de los ciudadanos europeos, en especial de su intimidad relativa a la información relacionada con su salud, se apunta la presencia de otros intereses generales como los estudios epidemiológicos, las situaciones de riesgo grave para la salud de la colectividad, la investigación y los ensayos clínicos que, cuando estén incluidos en normas de rango de Ley, pueden justificar una excepción motivada a los derechos del paciente. Se manifiesta así una concepción comunitaria del derecho a la salud, en la que, junto al interés singular de cada individuo, como destinatario por excelencia de la información relativa a la salud, aparecen también otros agentes y bienes jurídicos referidos a la salud pública, que deben ser considerados, con la relevancia necesaria, en una sociedad democrática avanzada. En esta línea, el Consejo de Europa, en su Recomendación de 13 de febrero de 1997, relativa a la protección de los datos médicos, después de afirmar que deben recogerse y procesarse con el consentimiento del afectado, indica que la información puede restringirse si así lo dispone una Ley y constituye una medida necesaria por razones de interés general".

Por último, el artículo 19 (Derechos relacionados con la custodia de la historia clínica) reza con el siguiente tenor: "El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la presente Ley".

En junio de 2003, la Junta Directiva de la Sociedad Española de Sanidad Pública y Administración Sanitaria (SESPAS), publicó un manifiesto[28] en defensa de la confidencialidad y el secreto médico que venía a resumir, de un modo muy adecuado quince cuestiones fundamentales de la protección de datos sanitarios. Se fundamentaba en una serie de postulados que reproducimos por su claridad, y que nos sirven como colofón en este apartado:

1. La intimidad es un valor ético y jurídico amparado por la Constitución y por la legislación vigente en nuestro país, y como tal hay que demandarlo y protegerlo por profesionales y usuarios.

2. El valor supremo de la vida y la defensa de la salud son motivo de que en la intimidad de la consulta médica se revelen secretos que no se confían ni siquiera a los más allegados; por eso la confidencialidad y el secreto médico son imprescindibles en la relación médico-paciente.

3. Los datos médicos pertenecen a cada paciente, y éste tiene todos los derechos sobre los mismos. El profesional sanitario, a quien el paciente se los confía, actuará como depositario, ejerciendo esos derechos como agente y responsable ante el paciente.

4. Los datos médicos son tan relevantes que si falla la confidencialidad no sólo está en peligro la intimidad, sino el ejercicio de otros derechos fundamentales, como el derecho al trabajo, a la educación, o la defensa de la salud y de la vida. El derecho a la confidencialidad que tiene todo paciente es la única garantía para la defensa de su intimidad.

5. El paciente tiene el derecho a ser informado de un modo que pueda comprender: acerca del responsable, destino y uso de sus datos personales; a que se requiera su consentimiento previo para la recogida y utilización de los datos, y el derecho a acceder, rectificar y cancelar dichos datos; en definitiva, el paciente tiene autonomía y poder de disposición sobre sus datos personales. Como establece el Tribunal Constitucional, todo paciente tiene el derecho fundamental a la protección de sus datos de carácter personal, que persigue garantizar un poder de control sobre los datos, su uso y su destino.

6. El secreto es un deber del médico y un derecho del paciente. El secreto médico se ha de proteger en el tratamiento de los datos sanitarios, ya sea en medios manuales o informatizados, como se establece en la legislación vigente, exigiendo las medidas de seguridad apropiadas que garanticen la protección de los datos personales de los pacientes. Sin estas medidas de seguridad no se deberán tratar los datos de salud.

7. Sólo en contadas ocasiones y bajo el imperio de la Ley, el derecho a la confidencialidad puede subordinarse a otras consideraciones. El allanamiento de la intimidad, como el de la propia morada, sólo puede justificarse por derechos superiores de otros o el bien

[28] Sociedad Española de Salid Pública y Administración Sanitaria. Manifiesto en defensa de la confidencialidad y el secreto médico. Gac Sanit 2003;17(4):337-9.

común, como en el caso de la salud pública, pero debe tenerse en cuenta que, a diferencia de la morada y otros bienes, la intimidad perdida no se puede restituir.

8. En casi todas las ocasiones, el anonimato estricto es idéntico al secreto y los datos anónimos pueden cumplir casi todas las tareas de administración. Sólo contadas informaciones clínicas personalizadas son relevantes para la gestión clínica y ninguna es relevante para la gestión de la información misma, por lo que ninguna de estas excusas puede utilizarse para justificar el almacenamiento masivo o centralizado de información sanitaria personalizada.

9. La informatización de las consultas y la historia electrónica de salud constituyen un factor de progreso; no obstante, en su utilización deben considerarse los peligros para la confidencialidad de los datos, por su almacenamiento fácil de ocultar, su infinita capacidad de copia y transferencia, indetectable y de ínfimo coste, y sus ilimitadas posibilidades de procesamiento y cruce. No puede garantizarse que la protección de los datos médicos centralizados sea infranqueable, teniendo en cuenta que el interés y el valor de tanta información son elevados: basta una única fuga, en un único punto para que los daños sean catastróficos e irreparables. El almacenamiento masivo centralizado de la información clínica es el que mayores riesgos supone para el secreto y la confidencialidad, comparando con las bases de datos distribuidas. Deben por tanto primarse soluciones tecnológicas pequeñas y repartidas, ya posibles, que eviten tan elevado riesgo.

10. La concentración de datos los hace codiciables, por lo que deben existir razones irrefutables para justificar el almacenamiento masivo o centralizado de información. La amenaza a la confidencialidad así creada, exige una total transparencia en este tipo de iniciativas, sancionadas por el consenso de grupos independientes (científicos, profesionales, judiciales, políticos, ciudadanos, económicos y comerciales) en cuanto a la pertinencia y relevancia de los datos precisos.

11. También debe determinarse –en la fase previa a toda implantación de almacenamientos masivos o centralizados– el tiempo de almacenamiento y las garantías y medios de destrucción irreversible de la información y todas sus copias, una vez cumplida su función.

12. Los sistemas pequeños y repartidos permiten proteger la confidencialidad, la intimidad de los pacientes y el secreto médico, como establece el Código de Deontología Médica; los sistemas de informatización médica tendrán implantadas las medidas de seguridad necesarias que eviten que otras personas accedan a los datos de los pacientes. Asimismo, todos los ficheros con historias clínicas y datos de salud estarán bajo la responsabilidad de un médico, y los ficheros con datos sanitarios no deberán conectarse a redes no médicas, como algunas redes institucionales. Esto, actualmente, no se respeta.

13. Es necesario establecer una legislación propia para proteger la intimidad de los pacientes, que nadie pueda ser discriminado por información relativa a la salud y la salvaguarda del secreto médico, en desarrollo específico de los artículos 14 y 18 de la Constitución. Es vital que la salud de una persona y los datos relativos a la misma nunca puedan ser usados en su contra o para su discriminación, sean o no sus depositarios «legítimos».

14. Es necesario que todos los ciudadanos defiendan y requieran el secreto médico a los profesionales sanitarios que les atienden. La legislación es importante, pero han de ser los propios pacientes los que exijan su derecho a estar informados sobre qué se hace con sus datos, a decidir quién los maneja y a defender el secreto médico.

15. El secreto es asimismo una prerrogativa del médico, manifestación de su derecho a la objeción de conciencia en las relaciones administrativas, profesionales o de cualquier otra.

III. ESTUDIO PRÁCTICO DEL ACCESO AL APLICATIVO "SELENE" POR FACULTATIVOS DEL SERVICIO MURCIANO DE SALUD

III.1 *El aplicativo SELENE*

El programa informático SELENE es la estación clínica del Sistema de Información Corporativo del Servicio Murciano de Salud (SMS). Comenzó a implantarse en los hospitales a mediados de la década de los 2000[29]. Es una solución clínica integral que gestiona el proceso asistencial completo. El proceso asistencial en SELENE refleja cada una de las relaciones del paciente con el sistema sanitario. Esta relación se visualiza de forma unificada aunque se produzca en diferentes lugares y momentos (primaria, hospital, centro de especialidades, ambulancia, etc.)[30].

La perspectiva sobre la que se enmarca SELENE parte del planteamiento de un concepto de Sistema de Informatización como verdadero almacén de conocimiento que integre todos los flujos de trabajo y los flujos de información dentro del Área de Salud. Trata pues de constituir una solución orientada a la integración de las actividades de todos los roles que participan en la asistencia al paciente en un Sistema de Información Sanitario completo y homogéneo, orientado a la eficiencia de los procesos, la mejora de los flujos de trabajo, la reducción de costes operativos y, sobre todo, la mejora de la calidad asistencial. La arquitectura de integración soportada en SELENE permite la interacción con todo tipo de sistemas clínicos (como los sistemas departamentales de laboratorio, radiología, etc. o software de dispositivos electrodomésticos) así como herramientas financieras.

El diseño conceptual aquí planteado es realmente un modelo organizativo de procesos, exportable a otros entornos clínicos, orientado directamente a proponer una solución de integración de Áreas de Salud.

Se trata de una plataforma completa compuesta por varios módulos funcionales interrelacionados entre sí, con los que poder cubrir la demanda funcional y de acceso a la información en un entorno sanitario amplio y complejo, estando especialmente orientada a cubrir las necesidades de compartición de información y de servicios en un entorno de Comunidad, en el que están implicados varios ámbitos asistenciales (Atención Especializada, Servicios de Emergencias, Salud Mental, Socio-Sanitarios), que podrán funcionar con la Plataforma SELENE o con cualquier otra aplicación.

Para el acceso a toda esta información, al usuario se le requiere un password y un login de acceso. Se definen varios grupos de usuarios que disponen de los mismos permisos sobre el

[29] SANCHEZ ROS, N., REIGOSA GAGO, L.F., "Selene. Informatización de la historia clínica electrónica: implicación sobre el proceso de enfermería". *Enfermería Global*, 2006. Pág. 2. www.um.es/eglobal

[30] © SIEMENS Medical Solutioes Health Services, 2007-All right reserved

sistema, se relacionan en los mismos circuitos y por lo tanto deben acceder al mismo grupo de información. Las propiedades asociadas a cada grupo de usuarios son administrables, de forma que se establecen categorías y niveles de acceso con distinta capacidad de tratamiento de datos.

Estos niveles bien definidos en teoría, y los niveles de seguridad a la hora de acceder a la historia clínica, presentan sin embargo en la práctica ciertas dificultades que podrían perjudicar seriamente la confidencialidad de la historia clínica. La clave de acceso requiere 5 caracteres únicamente, no precisa incluir ningún número, es válida durante 6000 días, el período de antelación con el que se avisa de la inactivación son 30 días, y el tiempo máximo que se puede estar sin usar previo a su inactivación automática son 45 días. De tales medidas de seguridad se desprende, que el acceso a la historia clínica, en aras de facilitar su establecimiento entre el personal sanitario, es, en exceso débil desde el punto de vista de la confidencialidad. A nadie se le escapa examinando las características exigidas para la adquisición de una clave que, no sólo son fácilmente memorizables e incluso deducibles (la clave asignada para la gran mayoría de los usuarios actualmente siguen siendo las iniciales de cada sujeto mas las dos últimas cifras de DNI junto a la letra de este para el usuario, y lo mismo para el login), sino que además son válidas durante al menos 6000 días, sin que el sistema obligue al cambio de clave de forma frecuente o periódica.

Y, no sólo eso. En la práctica clínica, la probabilidad de incurrir en accesos erróneos o ilegales a los historiales médicos, se multiplica en tanto más grande es el número de personas con capacidad para acceder al sistema. Dado el voluminoso número de contratados en un hospital como el que nos ocupa, podemos imaginarnos la cantidad de personas que tienen acceso a numerosos datos acerca del estado de salud de los pacientes

III.2 *El estudio práctico. Objetivo. Material y Métodos.*

Con el fin de aplicar los conceptos teóricos de protección de datos a la práctica diaria del facultativo, se planteó la realización de un estudio de investigación cuyos objetivos se resumían en los siguientes:

- Evaluar el grado de protección en el tratamiento de los datos clínicos informatizados en un medio hospitalario.
- Proponer medidas para preservar y mejorar la privacidad en el tratamiento de los datos.

El medio elegido para realizar el estudio fue el Hospital Clínico Universitario "Virgen de la Arrixaca", centro sanitario de la Región de Murcia, catalogado de tercer nivel, dotado de 873 camas y que atiende a una población aproximada de 426.661 personas, siendo hospital de referencia para toda la Región de Murcia en diversas especialidades médico/quirúrgicas, tales como Neurocirugía, Unidad de Quemados, Cirugía Cardiovascular y Unidad de Trasplante (médula ósea y órgano sólido).

El total de facultativos especialistas de área (FEA) es de 702 (incluyendo aquí los jefes de departamento, sección o servicio), y 297 médicos internos residentes (MIR) de 297.

Para la realización del estudio se ha llevado a cabo la difusión de encuestas sobre la población a estudio, limitada para este trabajo al personal facultativo por ser éste el que posee un acceso ilimitado a los datos sanitarios. El tamaño muestral necesario para obtener resultados estadísticamente significativos fue de 70 encuestas para los FEA y de 30 para los MIR. Finalmente se realizaron 80 encuestas entre el personal FEA y 33 entre el personal MIR.

El cuestionario constaba de 10 preguntas, ocho de ellas con una variable dicotómica de respuesta, otra con una variable de satisfacción entre bajo-medio-alto, y finalmente una pregunta abierta. Los resultados fueron evaluados según tablas de frecuencia y, para la comparación entre población de médicos adjuntos con médicos residentes, mediante la prueba de chi-cuadrado.

III.3 *Resultados*

Globalmente, de los resultados obtenidos se desprende que el 66.7% de los facultativos encuestados consideran "medio" el nivel de satisfacción con el sistema SELENE en la práctica clínica, siendo considerado "alto" por un 22,5% de la misma población.

Hasta un 77,5% de los facultativos reconocen haber accedido alguna vez al historial de un paciente que no fuera suyo, y hasta un 35% dice haber accedido alguna vez al sistema con una clave que no fuera la suya. El 89,2% de los encuestados reconoce así mismo haber dejado alguna vez el programa abierto con su clave en algún ordenador, y hasta el 52,5% admite haber cedido su clave alguna vez a otros (otro FEA, otro MIR, enfermeras, administrativos…).

El 55% de los facultativos considera que se debe tener acceso a cualquier historial clínico, y hasta el 68,3% de los encuestados considera que no es seguro el acceso a la historia clínica electrónica. El 69,2% de los facultativos considera insuficiente el control en la identificación a la hora de acceder a los historiales clínicos, y hasta un 67,5% establecería controles más rigurosos en este sentido.

En relación a las diferencias en ambos grupos encuestados (FEA vs MIR), y en cuanto al grado de satisfacción del personal sanitario facultativo con el programa SELENE (pregunta 1), un 12.8% de los FEAS (facultativos especialistas de área) lo calificaron como bajo, mientras que entre los residentes lo calificaron como bajo sólo el 5,9%. Se consideró como medio el nivel de satisfacción del 68,6% de los FEAS y del 61,8% de los MIR (médicos internos residentes). En total, el 66,7% de la población señaló el grado de satisfacción en nivel medio, si bien este resultado no fue estadísticamente significativo (p= 0,193).

En la pregunta 2, acerca de si alguna vez se ha accedido al historial de algún paciente que no fuera propio, el 74,4% del total de los FEAS reconoció haberlo hecho, mientras que este porcentaje ascendió hasta el 85,3% entre los MIR (p= 0,199). En total, el 77,5% de la población estudiada fue consciente de haber consultado el historial clínico de pacientes que no le habían sido asignados.

En relación a la pregunta 3, sobre si alguna vez se hubiera accedido al programa con una clave distinta de la propia, una mayor representación de FEAS (72,1%) dijo que no, mientras que hasta un 52,9% de los MIR reconoció que sí. Esta asociación resultó estadísticamente significativa (p=< 0,010*).

Sobre la pregunta 4, acerca de si alguna vez se hubieran dejado el programa abierto con su clave en un ordenador, hasta el 84,9% de los FEAS y el 100% de los MIR reconocieron haberlo hecho alguna vez, siendo dichas asociaciones estadísticamente significativas (p=0,016*).

La pregunta 5, acerca de si alguna vez se hubiera cedido la clave propia a otra persona (MIR, administrativo, personal de enfermería…), obtuvo un 55,8% de respuestas afirmativas entre los FEAS y un 44,1% del personal MIR, no siendo esta relación estadísticamente significativa (p>0,05).

Sobre si se considera que un facultativo debe tener acceso a cualquier historia clínica (pregunta 6), con una asociación no estadísticamente significativa, se valoró que sí en el 55% del total de la población estudiada, siendo que no en hasta 46,5% del personal FEA y en un 41% del personal MIR. (p=0.597).

Acerca de la pregunta 7, en relación a si se considera seguro el acceso a la historia clínica electrónica, un 68,3% de los encuestados respondió que no. Entre los MIR, el 76,5% cree que no es seguro el acceso, mientras que entre los FEA no lo considera seguro el 65,1%. Pese a encontrarse tendencia, esta asociación no fue estadísticamente significativa.

Muy relacionada a esta cuestión, la pregunta número 8 versaba sobre si se considera suficiente el control de acceso a la historia clínica. En este caso, en un porcentaje muy similar entre ambas poblaciones se consideró que no (67,6% de los MIR, 69,8% de los FEA). Tampoco en este caso la asociación fue estadísticamente significativa.

Finalmente, en cuanto a si se establecería controles más rigurosos en el acceso o identificación del facultativo a la hora de acceder a la historia clínica, un 73,3% de los FEA y un 52,9% del personal MIR consideró que sí, alcanzándose la significación estadística (p=0,032).

Para concluir, con respecto a la pregunta 10, que era una pregunta abierta acerca de las posibles mejoras en el sistema, se advierte una cierta tendencia en puntos clave como la rapidez del sistema y en la necesidad de mejora de perfiles profesionales. Otras medidas contempladas repetidamente por el personal sanitario encuestado fueron la necesidad de mejorar la seguridad con respecto a la intimidad, mejoras en la simplificación a la hora de manejo del sistema y el acceso a los historiales de otras áreas (recordemos que el hospital es considerado de referencia en la región para diversas especialidades).

III.4 *Discusión*

Las consecuencias de la informatización, buenas y malas, se sufren tanto por parte de los usuarios como de los profesionales en el día a día. Éstos han precisado de una *reeducación* básica en el uso de las nuevas tecnologías cambiando por completo tanto la forma de utilizar los servicios médicos en lo concerniente a los usuarios, como en la forma de ejercer los cuidados sanitarios (cuidados médicos, de enfermería, farmacia…) por parte de los profesionales.

Esta nueva concepción (o mejor, renovación del concepto) de medicina y asistencia sanitaria, tiene sin duda grandes fortalezas tales como la mayor disponibilidad y acceso a los datos tanto desde los servicios de urgencias como desde otros puntos geográficos, una mejor legibilidad, agilidad de la asistencia sanitaria, mejor gestión al evitarse pruebas innecesarias etc. Además, también ofrece verdaderas oportunidades en cuanto a una mayor equidad e interconexión de los distintos sistemas sanitarios, mayor gestión de calidad y planificación sanitaria, y facilita en gran medida la investigación y la evaluación del sistema.

Pero la implantación de las nuevas tecnologías no es gratuita. El precio a pagar, no sólo económico, sino en cuanto al aprendizaje del funcionamiento y sus posibles peligros asociados no es tema baladí. Frente a los problemas de formación del personal (y de los usuarios), el entorpecimiento de la actividad asistencial que muchas veces supone el acceso a los datos mediante rigurosos (o no tanto) procesos de identificación, se encuentra la posible deshumanización en la práctica clínica, la arriesgada dependencia que se genera sobre un único

sistema, y la cada vez más en boga posible violación de intimidad y privacidad sobre el tratamiento de los datos, con el cuestionado uso que se pueda hacer de ellos.

Atendiendo a los datos que se derivan del análisis de los resultados de las encuestas, llama la atención a priori, el alto porcentaje (77,5%) de facultativos que alguna vez accedieron al historial de pacientes de los que no eran médicos responsables, lo que equivale prácticamente a las tres cuartas partes de la población médica. Muchas veces, estas consultas pueden responder a colaboraciones entre los propios colegas durante la puesta en común de un caso, estudios o investigación. Otras veces puede deberse a que un facultativo se encuentre de guardia y, por tanto, deba acceder a estos historiales en el contexto de una urgencia, o, que no siendo el médico responsable, forme parte del mismo equipo y deba dar algún tipo de información puntual al paciente en ausencia de un compañero. Más controvertidos son los casos de los familiares o allegados del propio médico a cuyos datos tendrá acceso éste con la presunta autorización del paciente. En cualquier caso, creemos que previo al acceso, se debería tratar de dejar reflejada la razón que lleva a la búsqueda en cuestión.

Como vimos en los resultados, también en un alto porcentaje (89%), el personal médico reconoce haberse dejado el programa abierto con su clave en un ordenador (84,9% de los FEAS y el 100% de los MIR (p=0,016).) Este hecho, tan frecuente en la práctica clínica por la necesidad de consultar informes o reflejar los datos que se recogen en un momento determinado en pacientes situados en distintas plantas, responde muchas veces a la falta de conciencia de estar ejerciendo una "amenaza potencial" sobre la intimidad de los pacientes al dejar una puerta de acceso por parte de cualquier otra persona, médico o no, al historial clínico de todos los pacientes que haya registrados en la base de datos. Llama la atención además, la diferencia estadísticamente significativa que encontramos en relación al acceso al sistema con una clave distinta de la propia, que entre los FEAS representó un porcentaje mucho menor (27,9%) que entre los MIR (52,9%), lo que podría suponer una mayor conciencia de lo personal e intransferible que deberían resultar dichas claves entre el personal de mayor experiencia. En relación a esto hechos, consideramos que es precisa la concienciación del personal facultativo sobre el cuidado de las propias claves mediante conferencias o cursos que, en vista de los resultados entre el personal MIR deberían impartirse a su llegada al hospital.

Parece sin embargo unánime por parte el personal facultativo (70%) la consideración de que las medidas actuales de control de acceso son insuficientes y que existe una necesidad de establecer mayores controles en el acceso o identificación del facultativo a la hora de acceder a la HC; así lo cree un 73,3% de los FEA y un 52,9% del personal MIR (p=0,032), lo que hace pensar que el propio personal advierte la precariedad en los sistemas de identificación.

Hay mayor divergencia en cuanto a la opinión sobre si un facultativo debe tener acceso a cualquier historia clínica, ya que hasta el 55% del total de los médicos opina que sí. Pese a que son mayoría, existe una gran parte del sector que creen que sólo debería tener acceso el médico responsable en cada momento y los miembros de su equipo. Esta opción podría sin embargo acarrear problemas y enlentecimiento en la práctica habitual dada la interdisciplinaridad con la que cuenta hoy día el manejo de enfermedades y que en muchas ocasiones, sobre todo en el ámbito hospitalario, precisa de la consulta e intervención de diversas especialidades a diario.

En cuanto a las posibilidades de mejora del sistema, se advierte que lo que más preocupa al sector médico en relación a SELENE, es la rapidez y la mejora del los perfiles profesionales, lo que parece lógico, dado que se trata de lo que determina la fluidez en el trabajo. También se valoró repetidamente la necesidad de establecer mayores controles de seguridad, por lo que parece que cada vez se es más consciente de los peligros que acechan a la

confidencialidad, y en la simplificación del manejo del sistema así como el acceso a los historiales de otras áreas, lo cual está en gran medida influenciado por tratarse de un hospital de referencia en la región.

En relación con las características actuales de las claves de acceso al sistema SELENE, como ya se comentó más arriba, parecen insuficientes las medidas exigidas, y existen verdaderos problemas derivados de la simplicidad en dichas claves, ya que son sencillas de recordar y en muchos casos deducibles. Además, el tiempo de validez es largo (6000 días, lo que supone un total de > de 16 años) y no existe en el momento actual ninguna periodicidad obligatoria en el cambio de clave de seguridad. Otro dilema añadido es el de la validez de las claves para el personal contratado que sigue siendo vigente tras cumplirse el contrato, inhabilitándose únicamente de manera automática a los 45 días de la ausencia de actividad. La cesión de las claves, que es, como se desprende de la encuesta, una práctica no poco habitual, incurre también en un riesgo de perversión del sistema, ya que si bien queda reflejada la fecha, la hora y el terminal desde el que se ha accedido a un historial clínico, estas medidas parecen insuficientes no sólo por tratarse de medidas que toman valor si se prueba el daño, sino porque es difícil probar qué persona y con qué finalidad fue la que accedió a determinados datos del historial. Parece insólito, que en lo referido a datos de salud, considerados más sensibles que los datos fiscales por ejemplo, no se establezcan medidas de seguridad más complicadas y difíciles de descifrar, tal y como ocurre entre los funcionarios de Hacienda. Si bien el modo de trabajo es distinto, y es precisa, como se señalaba más arriba, en numerosas ocasiones la colaboración entre distintas personas para el desarrollo del trabajo, parece evidente que la falta de concienciación de la "potencialidad" de las claves es un hecho en el ámbito hospitalario.

Con respecto a una situación ideal, que en relación a la encuesta sería que se accediese siempre por un motivo justificado a determinado historial, que nunca se cedieran las claves a otros facultativos o a otros perfiles profesionales sanitarios o administrativos, que nunca se accediera con una clave distinta a la propia o que se implementen mayores medidas de seguridad en el sistema, vemos, a la luz de los resultados que aún nos queda mucho camino por recorrer.

Por último, en cuanto a la normativa, en el ordenamiento jurídico español carecemos de un marco legal de los datos sanitarios que afectan a las personas que responda, de manera integral, a los derechos fundamentales del paciente y del profesional para asegurar las necesarias garantías en el tratamiento de esta información y buscando el justo equilibrio que garantice todos los derechos implicados.

Atendiendo concretamente al programa SELENE, en nuestra comunidad autónoma, no existe una norma que regule su uso, si bien se le menciona indirectamente en otras. Asímismo, también encontramos referencias a SELENE en diversos artículos publicados, pero en ningún caso se trata de normas obligatorias[31].

Probablemente sería conveniente elaborar alguna instrucción capaz de regular, tal y como sucede en el modelo gallego, la utilización de la historia clínica electrónica, su implantación y el uso de las nuevas tecnologías de la información en el acceso y elaboración de la historia clínica, para constituir la base de una información sanitaria de mayor calidad y más segura.

[31] REIGOSA GAGO, L.F., "Selene. Informatización de la historia clínica electrónica: implicación sobre el proceso de enfermería". *Enfermería Global*, 2006. www.um.es/eglobal

Partiendo de una situación ideal en la que debería primar el acceso incorruptible a la historia clínica, se extraen una serie de medidas para tratar de asegurar un mayor grado de responsabilidad y concienciación a la hora del uso de SELENE. El proyecto de mejora será medible tras su implantación a través de la recogida de encuestas para ver en qué grado se consigue optimizar la confidencialidad de la historia clínica electrónica. Así:

a) Cursos/sesiones de confidencialidad de la historia clínica y valoración de las claves de acceso al programa informático SELENE. Estos cursos debieran impartirse a los MIR de primer año a su entrada al hospital, y periódicamente en los diversos servicios.

b) Mayor control en la identificación de todo profesional que intente acceder a la información mediante la verificación de la autorización de que se dispone.

c) Medidas técnicas y operativas de control de acceso de los profesionales a la información mediante el uso de una tarjeta identificativa del profesional y su firma electrónica

d) Auditorías internas de SELENE

e) Elaboración de una normativa aplicada específicamente al manejo de la historia clínica en SELENE.

IV. CONCLUSIONES

- La historia clínica electrónica se constituye como el soporte más adecuado para la asistencia sanitaria, facilitando el manejo y la accesibilidad de la documentación clínica del /de la paciente o usuario/a y a cuyo objeto los profesionales que intervienen en ella tienen el derecho de acceso y deber de acceder y cumplimentar la historia clínica electrónica.

- En el ordenamiento jurídico español carecemos de un marco legal de los datos sanitarios que afectan a las personas que responda, de manera integral, a los derechos fundamentales del paciente y del profesional para asegurar las necesarias garantías en el tratamiento de esta información y buscando el justo equilibrio que garantice todos los derechos implicados.

- Es preciso regular algunos aspectos referidos al manejo electrónico de la información personal por parte de las instituciones asistenciales públicas y personales, estableciendo totales garantías de confidencialidad e integridad de los datos.

- En la práctica clínica asistencial en el medio estudiado (HCUVA), existe, a la vista de los resultados de las encuestas, una clara falta de concienciación a la hora del acceso a la historia clínica electrónica a través del programa SELENE.

- Se precisa de la instauración de medidas de control más rigurosas para preservar la confidencialidad con mayor garantía en la práctica clínica habitual, a través de un programa de mejora que incluya la impartición de cursos, mayor control en la identificación del profesional o auditorías del programa SELENE.

V. REFERENCIAS BIBLIOGRÁFICAS

- ABERASTURI GORRIÑO, U., *La Protección de Datos en la Sanidad*, ed. Aranzadi, Navarra, 2013.
- ANTOMÁS, J., HUARTE DEL BARRIO, S. "Confidencialidad e historia clínica. Consideraciones ético-legales", *An. Sist. Sanit.*, 2011.
- BELTRÁN, J.L., "Tratamiento de datos de salud en la prestación de servicios sociales", *Derecho y Salud*, 2009; 18 (1): 1-19.
- BELTRÁN, J.L., *La protección de datos personales relacionados con la salud*. Ponencia del Defensor del Pueblo de Navarra, (27 de junio de 2012).
- BELTRÁN, J.L., COLLAZO, E., GERVÁS, J., *Intimidad, confidencialidad y secreto*, Madrid, ed. Ergon, 2005. Navarra, 2013.
- CÁLIZ CÁLIZ, R., *El derecho a la protección de datos en la historia clínica y la receta electrónica*, Thomson Renters, Navarra, 2009, pp. 35-46.
- CARNICERO GIMÉNEZ DE AZCÁRATE, J., *El derecho a la protección de datos en la historia clínica y la receta electrónica*, ed. Aranzadi, Navarra, 2009, pp. 309-310.
- CORBELLA, J., *Manual de Derecho Sanitario*. Barcelona: Atelier Libros S.A, 2ª ed., 2012.
- DEL PESO NAVARRO, E., *La seguridad de los datos de carácter personal*, ed. Díaz de Santos, Madrid, 2002.
- GÓMEZ SÁNCHEZ, Y., "Datos de salud como datos especialmente protegidos. Título II. Principios de protección de datos. Artículo 7", TRONCOSO REIGADA, A. (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, Civitas, pp. 647-671.
- GONZÁLEZ GARCÍA, C., *La Protección de Datos Personales en el Ámbito Sanitario*, ed. Aranzadi, Navarra, 2002, p.111.
- LARIOS, D., SÁIZ, M., "El derecho de acceso a la historia clínica por el paciente: propuesta para la reserva de anotaciones subjetivas", *Derecho y Salud*, 2009, 18 (1): 21-41.
- REIGOSA GAGO, L.F., "Selene. Informatización de la historia clínica electrónica: implicación sobre el proceso de enfermería". *Enfermería Global*, 2006. www.um.es/eglobal
- SÁNCHEZ-CARO, J., "La historia clínica electrónica gallega: un paso importante en la gestión del conocimiento" Dir. D.L.R., *Derecho y salud*, Santiago de Compostela, 2001, p. 57
- SÁNCHEZ-CARO, J., *El médico y la intimidad*, Ed. Díaz de Santos, Madrid, 2001.
- SÁNCHEZ ROS, N. y REIGOSA GAGO, L.F., "Selene. Informatización de la historia clínica electrónica: implicación sobre el proceso de enfermería". *Enfermería Global*, 2006, p.2 www.um.es/eglobal
- SIEGLER, M., "Confidentiality in medicine. A decreipt concept", *The New England Journal of Medicine* 1982, pp. 1518-1521.

- TRONCOSO, A., *La protección de datos personales. En busca del equilibrio*. 1ª ed. Valencia: Tirant Lo Blanch, 2010.

OTRA DOCUMENTACIÓN CONSULTADA

- Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos. Grupo de Trabajo sobre protección de datos del artículo 29. http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083. Fecha de acceso: 5-04-2018.
- Recomendación núm. 5, de 13 febrero 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos. http://www.coe.int
- Sociedad Española de Salud Pública y Administración Sanitaria. Manifiesto en defensa de la confidencialidad y el secreto médico. Gac Sanit 2003; 17(4): 337-9.

LEGISLACIÓN

- Constitución Española de 27 de diciembre de 1978. Boletín Oficial del Estado, núm. 311, p. 29313, (29 de diciembre de 1978).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE de 4 de mayo de 2016).
- Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al honor, a la intimidad personal y familiar y a la propia imagen. Boletín Oficial del Estado, nº 115, p. 12546, (14 de mayo de 1982).
- Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical. Boletín Oficial del Estado, nº 189, p. 16660, (8 de agosto de 1985).
- Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales de salud Pública. Boletín Oficial del Estado, nº 102, p. 15207, (29 de abril de 1986).
- Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Boletín Oficial del Estado, nº262, p. 37037, (31 de octubre de 1992).
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado, núm. 281, p. 33987, (24 de noviembre de 1995).
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado nº 298, p. 43088, (14 de diciembre de 1999).
- Ley 14/1986, de 25 de abril, General de Sanidad. Boletín Oficial del Estado, nº 102, p. 15207, (29 de abril de 1986).

- Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. Boletín Oficial del Estado, nº 75, p. 9654, (29 de marzo de 1995).
- Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales. Boletín Oficial del Estado, nº 269, p. 32590, (10 de noviembre de 1995).
- Real Decreto 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención. Boletín Oficial del Estado, nº 27, p. 3031, (31 de enero de 1997).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Boletín Oficial del Estado, nº 17, p. 4103, (19 de enero de 2008).