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

# MECANISMOS DE PREVENCIÓN DEL ACCESO INDEBIDO A LA HISTORIA CLÍNICA POR PARTE DEL PERSONAL SANITARIO Y NUEVA LEGISLACIÓN DE PROTECCIÓN DE DATOS

ANDREA SALUD CASANOVA ASENCIO

Contratada Predoctoral FPU-MECD
Universidad de Murcia[1]
acasanova@um.es

**RESUMEN:** El acceso injustificado a la historia clínica por parte del personal sanitario es un problema práctico de marcada incidencia en la actualidad, que no ha conseguido resolverse a pesar de los avances de los últimos años en materia de historia clínica. Al mismo tiempo, la nueva legislación de protección de datos (RGPD y la nueva LOPDGDD) supone un cambio en el modelo de seguridad de los mismos, al requerir una responsabilidad proactiva por parte del responsable del tratamiento, que deberá estudiar el riesgo al que los datos están sometidos por dicho tratamiento con el fin de adoptar las medidas técnicas y organizativas más adecuadas para garantizar la seguridad de los datos ya desde el propio diseño del sistema. Con esta perspectiva, se realiza una exposición y análisis de una serie de mecanismos preventivos de diverso tipo que, aplicados en conjunto, habrían de ser útiles para gestionar de mejor manera el problema de los accesos indebidos a la historia clínica por parte del personal sanitario sin vinculación asistencial.

**PALABRAS CLAVE:** historia clínica, datos de salud, acceso, personal sanitario, vinculación asistencial, confidencialidad, seguridad de los datos, Reglamento General de Protección de Datos.

**ABSTRACT:** Access to the medical history by health personnel that isn't justified by the supplying of the adequate health care –hence being deemed as an unjustified access- is currently a prominent practical problem which hasn't been solved despite the advance shown by medical history regulations in the last few years. At the same time, the new data protection regulation (GDPR and Spanish LOPDGDD) introduces a new model for the security of the data, emphasizing what is known as "accountability" by the controller of the data, which translates into data protection by design and by default. From this perspective, a series of preventive mechanisms to avoid unjustified access to a medical history is analysed and presented, assuming that the problem requires the joint application of at least several of these preventive tools.

**KEYWORDS:** medical history, health data, data access, health personnel, health care, confidentiality, data protection, General Data Protection Regulation.



[1] Financiación otorgada por el Ministerio de Educación, Cultura y Deporte de acuerdo con la Resolución de 19 de noviembre de 2015, por la que se convocan Ayudas para la Formación de Profesorado Universitario.

## I. EL ACCESO INJUSTIFICADO A LA HISTORIA CLÍNICA POR PARTE DEL PERSONAL SANITARIO. SU INCIDENCIA PRÁCTICA

Los datos contenidos en la historia clínica se caracterizan por su especial conexión con la intimidad de la persona[2], determinando que el mero acceso injustificado a los mismos sea capaz de irrogar un perjuicio para el interesado[3].

No en vano, estos datos son objeto de una protección especial por parte del Ordenamiento, como se ve en el artículo 7.1 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 (en adelante, LAP), que determina que nadie podrá acceder a los mismos salvo en los casos en los que concurra una finalidad legalmente prevista.

De entre las varias finalidades que el artículo 16 de la misma Ley recoge a tal efecto, destaca, por lo que aquí nos interesa, la conocida como "finalidad asistencial"; es decir, la relacionada con la prestación de asistencia sanitaria. Dice el artículo, así, que la historia clínica es "un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente", al que los profesionales han de poder acceder en cualquier momento a través del nuevo sistema de historia clínica electrónica[4], toda vez que se trata de un instrumento básico y

[2] No en vano, el propio artículo 7 de la LAP se sitúa bajo la rúbrica "Derecho a la intimidad"; un derecho reconocido constitucionalmente en el art. 18.1 CE y vinculado con la dignidad de la persona (SERRANO PÉREZ, M. M., "Salud pública, epidemiología y protección de datos", en Tratado de Derecho Sanitario, vol. I, Larios Risco, et al. (coord.), Thomson Reuters-Aranzadi, Cizur Menor, 2013, p. 1095).

A pesar de esta conexión, el derecho a la protección de los datos personales se considera incluido en el artículo 18.4 CE y se conceptualiza como un derecho autónomo respecto al derecho a la intimidad. Así lo indican el Preámbulo y el artículo 1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la jurisprudencia -tanto el Tribunal Constitucional (en la SSTC 254/1993, de 20 de julio (RTC 1993, 254) y otras), como el Tribunal Supremo (en la STS, Sala 2ª, nº 586/2016, de 4 de julio y otras que la citan)-, y, entre la doctrina, autores como GONZÁLEZ GARCÍA, L., "Derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos", Derecho y Salud, vol. 24, nº extra 1, 2014, p. 274 o, de manera más detallada, ORDÁS ALONSO, M., "Intimidad, secreto médico y protección de datos sanitarios", en Razonar sobre Derechos, García Amado, J. A. (coord.), Tirant lo Blanch, Valencia, 2016, pp. 780, 781 y 788 a 792).

[3] BARRAL comenta que, en este tipo de datos, al contrario de lo que sucede en relación a los datos ordinarios, el riesgo puede provenir directamente del contenido del dato (BARRAL, I., "Datos relativos a la salud e historia clínica: la confidencialidad de los datos médicos", en Protección de datos personales en la sociedad de la información y la vigilancia, Llácer Matacás, M. R. (coord.), La Ley, Madrid, 2011, p. 353).

[4] La implantación de la historia clínica electrónica trae un nuevo "escenario de integración y accesibilidad" (PEREIRA ÁLVAREZ, M., "El tratamiento de los datos en las HCE y las medidas de seguridad: una aproximación desde el punto de vista técnico. Especial Referencia al nuevo Reglamento de desarrollo de la LOPD", en El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica, Cáliz Cáliz, R. (coord.), et al., Thomson Reuters-Aranzadi, Cizur Menor, 2009, p. 309) que ha sido valorado de manera desigual por la doctrina en lo tocante a la seguridad de los datos. Así, mientras que para algunos autores supone un mayor riesgo desde el punto de vista de que ahora son más los usuarios que tienen un acceso potencial a los datos (como indican ORDÁS ALONSO, M., "Intimidad…", cit., pp. 774, 775; o el documento *Ética en el acceso y en el uso de la documentación clínica: reflexiones y recomendaciones*, 2017, del Consello de Bioética de Galicia); para otros supone una herramienta capaz de asegurar una protección de los datos mayor que la historia clínica en papel (en este sentido, pueden verse ETREROS HUERTA, J. J., "Historia clínica electrónica", en El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica, Cáliz Cáliz, R. (coord.), et al., Thomson Reuters-Aranzadi, Cizur Menor, 2009, p. 186; SÁNCHEZ CARO, J., "La historia clínica gallega: un paso importante en la gestión del conocimiento", Derecho y salud, vol. 18, nº 1, 2009, p. 58; o, también TRONCOSO REIGADA, A., "La confidencialidad de la historia clínica", Cuadernos de Derecho Público, nº 27, enero-abril 2006, pp. 84, 85, 137, 142, quien cree que, a pesar de que el traslado de los datos a soportes informáticos puede provocar mayores vulneraciones de derechos, es también la mejor manera de velar por la seguridad de los datos).

necesario en la prestación de servicios sanitarios[5], cuyo uso no sólo debe estar autorizado, sino que debe garantizarse, como se encarga de plasmar el artículo 16.2 LAP.

De esta forma, todos los accesos que se amparen en esta finalidad asistencial (lo que se conoce como *principio de vinculación asistencial*) estarían cubiertos por la autorización legal que supone el artículo 16.1 LAP, que además ha de completarse con el conocido como *principio de proporcionalidad*[6], que determina que únicamente sean consultados aquellos datos precisos para la concreta asistencia sanitaria que se va a prestar.

Sin embargo, no son pocas las ocasiones en que el personal sanitario accede sin estar cubierto por estos principios, actuando, en consecuencia, extramuros de la autorización legal del artículo 16 LAP. Estaríamos, entonces, ante un acceso ilegítimo o injustificado.

Pues bien: la incidencia práctica de los accesos injustificados a las historias clínicas por parte del personal sanitario es ciertamente mayor de la que se pueda imaginar. De hecho, llega a ser un problema práctico de gran magnitud.

Por dar sólo algunos de los datos posibles, podemos citar los que se manejan en el documento *Ética en el acceso y en el uso de la documentación clínica: reflexiones y recomendaciones*, preparado en 2017 por el Consello de Bioética de Galicia a propósito de la experiencia vivida en el sistema de salud de dicha Comunidad Autónoma tras la entrada en vigor del Decreto 29/2009, de 5 de febrero, por el que se regula el uso y el acceso a la historia clínica electrónica en Galicia, norma pionera que instaura un sistema -conocido como IANUS- que implementa un buen número de mecanismos y previsiones en pos del buen uso de la historia clínica y la supresión de las malas prácticas en torno a ella.

Los datos manejados por el Consello indican que la sospecha por parte de usuarios del sistema de salud de que terceros (familiares u otros) habían tenido acceso a sus datos clínicos es la causa más frecuente de reclamaciones ante la Inspección de servicios sanitarios de A Coruña, la cual, sólo entre abril de 2011 y abril de 2017, detectaba un acceso a la historia clínica en el 82% de los casos denunciados, 91% de los cuales no estaban justificados por una relación asistencial[7].

No es extraño, por tanto, que se hayan propuesto diversas soluciones al problema durante los últimos años. En concreto, el presente trabajo se centra en ofrecer una sistematización de los posibles mecanismos preventivos a adoptar frente al problema del acceso injustificado a la historia clínica por parte del personal sanitario, aunándose tanto algunas soluciones que ya han sido incorporadas a la práctica, como otras que sólo han sido esbozadas –o se esbozan aquí- en la teoría, en el entendimiento de que la problemática presentada requiere

[5] El Informe *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGDP* presentado por la Sociedad Española de Salud Pública y Administración Sanitaria en 2017 (en adelante, Informe SESPAS) tilda a la historia clínica como elemento necesario e inherente al tratamiento médico (p. 52). En el mismo sentido, autores como TRONCOSO REIGADA, que subraya su vinculación con los derechos constitucionalmente reconocidos a la vida (artículo 15 CE) y a la protección de la salud (artículo 43 CE) ("La confidencialidad…", cit., pp. 45, 46) e incluso indica que la confección de la historia clínica es un deber para todo profesional sanitario (p. 70), o GÓMEZ PIQUERAS, para quien la historia clínica es "el instrumento básico del buen ejercicio sanitario" (GÓMEZ PIQUERAS, C., "La historia clínica. Aspectos conflictivos resueltos por la Agencia Española de Protección de Datos", en El derecho a la protección de datos en la historia clínica y la receta electrónica, Cáliz Cáliz, R., et al. (coord.), Thomson Reuters-Aranzadi, Cizur Menor, 2009, p. 134).

[6] GONZÁLEZ GARCÍA, L., "Derecho…", cit., p. 277; SÁNCHEZ CARO, J, "La historia…", cit., p. 68; PEREIRA ÁLVAREZ, M., "El tratamiento…", cit., p. 311; Informe SESPAS, p. 53.

[7] P. 44 del documento del Consello. Vale la pena remarcar el hecho de que estos escandalosos datos son los recogidos en un territorio en el que existen ya algunas medidas avanzadas de prevención de accesos ilegítimos.

de una aplicación en conjunto de, como mínimo, varias de estas herramientas de manera simultánea para su eficacia.

## II. LA SEGURIDAD DE LOS DATOS DE SALUD EN LA NUEVA NORMATIVA DE PROTECCIÓN DE DATOS

Para hablar de los mecanismos de prevención de los accesos ilegítimos a la historia clínica, en la medida en que los datos de salud son, como se sabe, datos personales, es imprescindible tener presente el cambio de modelo que a efectos de la seguridad de los datos ha supuesto la aprobación del Reglamento de Protección de Datos[8] (en adelante, RGPD o Reglamento) y, con posterioridad, la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), que adapta el Ordenamiento español al Reglamento.

Esta nueva normativa de protección de datos se funda en un modelo basado en la responsabilidad proactiva de los responsables del tratamiento de los datos (art. 5.2 RGPD), los cuales deben incorporar medidas organizativas y técnicas que aseguren, desde el propio diseño de los ficheros y por defecto (esto último, en el sentido de asegurar que sólo sean objeto de tratamiento los datos que sean necesarios para el fin específico del tratamiento), la protección de los datos personales objeto del tratamiento, como disponen los artículos 24 y 25 RGPD, relativos a la responsabilidad del responsable del tratamiento y a la protección de datos desde el diseño y por defecto, respectivamente.

Este nuevo modelo, lejos de delimitar medidas o niveles de seguridad concretos, como hacía la normativa anterior, parte de la idea de que cada tratamiento concreto precisará de unas medidas de seguridad que se adapten al mismo. Puede verse, así, cómo el Reglamento habla de las "medidas adecuadas" o "apropiadas" en varias partes de su articulado y Considerandos.

En este sentido, el artículo 28 LOPDGDD se refiere a la obligación que tienen los responsables y encargados del tratamiento de determinar, teniendo en cuenta lo dispuesto por los artículos 24 y 25 RGPD, las medidas técnicas y organizativas apropiadas para garantizar y acreditar que el tratamiento es conforme con la legalidad vigente. Estas medidas deberán garantizar un nivel de seguridad adecuado al riesgo concreto que incluya, en todo caso, las salvaguardas previstas por el artículo 32.1 RGPD, debiéndose tener particularmente en cuenta los riesgos que presenten ciertas contingencias que pueden darse al efectuar el tratamiento de los datos, entre las que se contempla específicamente el acceso no autorizado a los mismos (art. 32.2 RGPD). Reflejo de este precepto es la Disposición Adicional primera de la LOPDGDD, que dispone que el Esquema Nacional de Seguridad incluirá las medidas a implantarse para evitar la pérdida, alteración, o, en lo que nos interesa, el acceso no autorizado a los datos personales.

Se ha de observar, además, que la falta de adopción de todas estas medidas de seguridad supone la comisión de infracciones de carácter grave, según se aprecia en el artículo 73 LOPDGDD.

Por otra parte, y para los supuestos que entrañen un alto riesgo para los derechos y libertades de las personas físicas, prevé el artículo 25 del Reglamento la obligación para el

[8] 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).

responsable del tratamiento de proceder a la evaluación del impacto de las operaciones de tratamiento en la protección de los datos personales[9]; cuestión a la que también se alude en el Considerando 83 del mismo texto.

Por su parte, la LOPDGDD concreta todavía más los casos en los que se habría de llevar a cabo esta evaluación de impacto al incluir, en el apartado segundo del artículo 28, una serie de supuestos que podrían entrañar un mayor riesgo a estos efectos[10], y entre los que se incluyen algunos que podrían ser predicables del tratamiento de datos de salud a propósito de la historia clínica[11], como son los que se señalan en la letra a), al hacerse referencia a la pérdida de confidencialidad de datos sujetos al secreto profesional, o en la c), relativo al tratamiento no incidental de datos a los que se refieren los artículos 9 y 20 RGPD, entre los que se incluyen los datos de salud.

Todas estas medidas de seguridad se completan, por un lado, con la previsión de la creación de códigos de conducta a los que los responsables y encargados del tratamiento pueden adherirse, los cuales se identifican por el Considerando 77[12] como directrices de "buenas prácticas para mitigar el riesgo" y aparecen regulados en general en los artículos 40 y 41 RGPD, así como, con previsiones más concretas, en el artículo 38 LOPDGDD, además de cobrar relevancia en otros aspectos de la regulación contenida por ambas normas[13].

Y, por otro, se establecen sistemas de certificación de cumplimiento con la legislación en materia de protección de datos (regulados en general en los artículos 42 RGPD y 39 LOPDGDD).

En último lugar, y como medida de cierre del sistema de seguridad, reviste gran importancia el deber de comunicar la violación de la seguridad (o "brecha de seguridad") de los datos (que incluye, como puede verse en el artículo 4.12 RGDP, el acceso no autorizado a los mismos) tanto a la autoridad de control (art. 33 RGDP), como, en algunos casos, al propio interesado (art. 34 RGDP), y de hacerlo, además, en el menor plazo posible[14], resultando, además, que la falta de esta comunicación supone la comisión de infracciones de diversa gravedad[15].

Una medida con carácter más reactivo que preventivo, puesto que adquiere virtualidad una vez se ha producido ya la violación de la seguridad de los datos (comúnmente denominada como "brecha de seguridad"), pero indudablemente efectiva, también, como elemento de

[9] No obstante, el Grupo de Trabajo del artículo 29 indica que no será preciso efectuar esta evaluación de impacto a operaciones de tratamiento ya existentes cuando las operaciones concretas hayan sido revisadas por una autoridad de control o delegado de protección de datos, en tanto en cuanto se realicen de una forma que no haya cambiado desde la anterior comprobación. A pesar de esto, las buenas prácticas imponen la necesidad de realizar esta evaluación debe ser continuamente revisada y reevaluada (Documento WP248, *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679*, en la versión revisada de 4 de octubre de 2017, pp. 15, 16).

[10] También se prevé que el responsable o encargado del tratamiento pueda considerar la conveniencia de realizar la evaluación de impacto en otros casos en los que pudiera ser aconsejable, según se desprende de la letra h) del artículo referenciado.

[11] El Grupo de Trabajo del artículo 29 da, precisamente, el ejemplo del hospital que guarda "historiales médicos de pacientes" (Documento WP248, p. 11).

[12] Este Considerando incluye, además, otras clases de indicaciones que pueden cumplir la función de mitigar el riesgo en el tratamiento de los datos.

[13] Por ejemplo, son relevantes a efectos de la responsabilidad del responsable y del encargado del tratamiento, como se ve en los artículos 25 y 28 RGPD, respectivamente, entre otras cuestiones.

[14] Es interesante, además, la motivación contenida en los Considerandos 85, 86 y 87 al respecto.

[15] Véase los artículos 73, letras q), r), s) y 74 ñ).

prevención, por el efecto disuasorio que para las entidades que realicen algún tipo de tratamiento de datos personales supone el hecho de que las quiebras en la seguridad no puedan pasar inadvertidas por imperativo legal.

Todo lo antedicho conformaría, así, el marco general que aporta la nueva legislación de protección de datos.

## III. MECANISMOS DE PREVENCIÓN DEL ACCESO ILEGÍTIMO A LA HISTORIA CLÍNICA

Como puede imaginarse, el nuevo modelo introducido por el RGDP y la LOPDGDD implica que las medidas de seguridad de carácter técnico y organizativo a aplicarse pueden ser reestructuradas si se considera que existen otras que puedan adaptarse mejor a las exigencias del nuevo sistema que las que ya se encuentran implantadas. No obstante, ello no quiere decir que no puedan mantenerse una gran parte de los mecanismos hasta ahora observados, en la medida en que sean eficaces para prevenir los accesos ilegítimos a la historia clínica.

A este respecto, mantiene su vigencia la previsión contenida en el artículo 14 LAP, que señala que es responsabilidad de cada centro archivar de manera segura las historias clínicas de sus pacientes, sea cual sea el formato, así como deber de las Comunidades Autónomas proceder a la aprobación de aquellas disposiciones que sean precisas para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para el archivo y la protección de las mismas.

Teniendo todo esto presente, se relaciona a continuación una serie de medidas preventivas, algunas extraídas de la práctica de los sistemas sanitarios, y otras que sólo han sido esbozadas –o se esbozan aquí– en la teoría, en el entendimiento de que la problemática presentada requeriría de una aplicación en conjunto de, como mínimo, varias de estas herramientas de manera simultánea para prevenir con eficacia los accesos injustificados a la historia clínica por parte del personal sanitario sin vinculación asistencial.

### III.1 *Formación en protección de datos y confidencialidad.*

El deber de confidencialidad es uno de los pilares básicos en la especial relación de confianza que se genera entre el paciente y los trabajadores sanitarios (en particular, en la relación médico-paciente[16]), y, bien observado, supone una serie de garantías para el paciente que se encuentra, muchas veces, en una situación de especial vulnerabilidad al comunicar sus datos de salud al profesional.

Por ello, no es extraño que un gran número de normas se encarguen de garantizar este deber. Así lo hacen los artículos 9.3 del Reglamento General de Protección de Datos (en una mención expresa bien acogida por la doctrina[17]), 10.3 de la Ley General Sanitaria[18], 7.1 LAP y

[16] Ésta era la relación de la que tradicionalmente se ha predicado el deber de confidencialidad. Sin embargo, y dado que el viejo modelo en el que un único facultativo atendía a las mismas personas durante toda la vida de éstas ha quedado superado, cabe decir que esta relación se ha visto, al menos en parte, sustituida por la que se da entre el paciente y el servicio de salud, lo cual no provoca menoscabo alguno del derecho a la intimidad de los pacientes, como ha determinado el Tribunal Constitucional en su Auto 600/1989, de 11 de diciembre.

[17] Informe SESPAS (p. 50).

16.6. LAP, pudiendo destacarse la previsión que realiza el artículo 2.7, que extiende el deber de confidencialidad a toda persona que tenga acceso a la documentación clínica, y no sólo, por tanto, a aquellos profesionales específicamente sujetos al deber de secreto profesional. Por otra parte, y fuera del ámbito sanitario, son relevantes el artículo 7.4 de la 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 en su artículo 7.4, que indica que tendrá carácter de intromisión ilegítima la revelación[19] de los datos conocidos a través de la actividad profesional de quien los revela, sin circunscribirse a aquellas profesiones sujetas específicamente a un deber de secreto profesional. Y, por otro lado, y de manera general, el artículo 5.1 LOPDGDD sujeta a los responsables y encargados del tratamiento de datos, así como a todos los que intervengan en cualquier fase del mismo, al deber de confidencialidad al que a su vez se refiere el artículo 5.1.f) del Reglamento, además de especificar que esta obligación general se verá complementada por los deberes de secreto profesional que deban observarse según la normativa aplicable en cada caso (artículo 5.2 LOPDGDD).

Como se ve, y al margen de la trascendencia del deber de confidencialidad en el ámbito de la deontología (véase que la práctica totalidad de Códigos Deontológicos le dan cobertura expresa, amén de establecer sanciones por incumplimiento del mismo), de este deber se ocupan expresamente la legislación en materia de protección de datos, la legislación sanitaria, e incluso otras normas del ámbito civil, como la LO 1/1982 dedicada a la protección de los derechos al honor, intimidad y propia imagen. No es sólo, por tanto, un deber deontológico, o *ético*, si así se le quiere llamar: es también un deber legal para el profesional sanitario.

Así las cosas, parece que una primera medida de prevención frente a los accesos injustificados a la historia clínica debe ser la recepción, por parte de los profesionales sanitarios, de formación específica en materia de confidencialidad en relación con el derecho de protección de datos[20]; formación que debe ser extensiva a todos aquéllos que, en mayor o menor medida, trabajen con este tipo de datos especialmente sensibles[21], y que debe estructurarse de manera que se integre tanto en el plan de acogida de nuevo personal, como, si es necesario, en sesiones periódicas para todo el equipo profesional que pueda entrar en contacto con dichos datos.

Puede añadirse la existencia de otros textos que apuntalan esta necesidad, como es el caso del Decálogo de la Historia Clínica aprobado en febrero de 2017 por la Comisión Central de Deontología de la Organización Médica Colegial de España y la Comisión Permanente del Consejo General de Colegios Oficiales de Médicos, que dispone la obligación para el médico de instruir en este deber deontológico a las personas que trabajen con él o que se encuentren en formación bajo su tutela.

La formación en materia de confidencialidad y protección de datos, en fin, se revela como imprescindible, y como la primera medida precautoria que probablemente deba tomarse para erradicar las malas prácticas en el acceso a la historia clínica. Sin embargo, hemos de ser conscientes también de que esta medida formativa, aunque necesaria, no es suficiente para

[18] Este artículo indica, como derecho de "todos" frente a las administraciones públicas sanitarias, el relacionado con "la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas", y además extiende esta previsión a todas aquellas entidades sanitarias privadas que colaboren con el sistema público.

[19] Si bien LO 1/1982 sólo comprende en su ámbito de aplicación la conducta compuesta por la revelación de los datos, y no el mero acceso a los mismos, del que ya hemos dicho que, en materia de datos de salud, puede constituir ya una conducta dañosa.

[20] También lo ha señalado la doctrina (*vid.*, por ejemplo, GONZÁLEZ GARCÍA, L., "Derecho…", cit., p. 278).

[21] Como hemos visto, el deber de reserva se extiende a todos ellos (art. 2.7 LAP).

prevenir todos los ataques a los datos personales de los pacientes, como la práctica demuestra[22], lo que nos ha de llevar, necesariamente, a otras soluciones preventivas a adoptar[23].

### III.2 *Implantación y utilización de software para la prevención y detección de posibles accesos injustificados.*

#### III.2.1 *Protocolos de acceso a los datos más eficaces.*

Hemos comentado antes que la normativa vigente en materia de protección de datos incide en la necesidad de establecer las medidas técnicas (y organizativas) adecuadas para asegurar la protección de los datos. A ello se refiere, también, la LAP en su artículo 17.6, al disponer que se aplicarán 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", remitiéndose también a la derogada LOPD (no obstante lo cual el artículo parece mantener total vigencia).

En relación a las medidas de seguridad en general, y bajo la vigencia de la ley anterior (aunque se entiende que lo dicho sería enteramente aplicable a la actual regulación), indicaban las Sentencias de la Audiencia Provincial de 13 de junio de 2002 y 7 de febrero de 2003 que estas medidas no habían de ser cualesquiera, sino las necesarias, y que además debían llevarse a cabo efectivamente; planteamiento que la nueva legislación no hace sino reforzar.

Como primera medida técnica de seguridad, cobran gran importancia los protocolos de acceso a los datos. A esta cuestión se refería el artículo 91 del Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007, de 21 de diciembre), haciendo referencia al sistema de control de accesos a los ficheros, al tiempo que el 93 del mismo texto se pronunciaba sobre la necesaria identificación y autenticación de los usuarios del fichero. Por otra parte, el RGPD también hace alguna referencia a esta cuestión, nombrando el control de accesos en su Considerando 126.

En cumplimiento de estas previsiones, los sistemas de seguridad aplicados a la historia clínica electrónica, en sus distintas variantes[24], permiten o deben permitir que sólo personal debidamente identificado pueda acceder, variando los distintos sistemas de identificación

[22] Viene a admitirlo también el documento elaborado por el Consello de Bioética de Galicia (pp. 44, 45).

[23] Ésta es la idea que subyace en la Sentencia del Juzgado de lo Contencioso-Administrativo nº 1 de Pamplona, nº 196/2011, de 25 de mayo (posteriormente confirmada por la STSJ Navarra nº 111/2012, de 8 de febrero), en la que se dilucida una reclamación contra el Servicio de Salud Navarro por el acceso masivo a la historia clínica de una paciente en estado de coma, en la que se incluía una serie de fotografías en las que podían apreciarse las graves lesiones que padecía, considerando que las medidas de seguridad establecidas eran claramente insuficientes. Dice expresamente la sentencia que el Servicio de Salud mentado "ha centrado su actividad en protección de los datos íntimos de los pacientes en fomentar la concienciación de los profesionales sobre la confidencialidad o secreto de los datos relativos a la salud de los usuarios más que en poner "barreras" efectivas a la accesibilidad de dichos datos, para evitar que el interés personal en unos casos, la curiosidad en otros o el chismorreo en otros más, se pongan por encima de la conciencia individual de los profesionales como, parece ser ha sucedido en el presente caso", comentando además que "esa carencia de sistemas de control en los accesos, y lo que ha permitido que con una razón o con otra, con una justificación o con otra, todo el que ha querido ha podido acceder, y de hecho ha accedido (…). Así, unos han accedido porque su hija había estado con la enferma, otros porque sus hijos son compañeros y otros, como lo reconoce algún sancionado, por puro "chismorreo", haciéndolo otros en grupos".

[24] Y es que, tratándose de una competencia autonómica, son distintos los sistemas aplicados en cada una de las Comunidades Autónomas, encontrándose cada uno de estos sistemas, además, en diferente estado de desarrollo. Sería deseable, como indica GÓMEZ PIQUERAS, una mayor unificación en esta materia ("La historia…", cit., p. 134).

empleados, que deben asegurar la suficiente accesibilidad (no debiendo adolecer, por tanto, de excesiva complejidad), pero sin poner en peligro la seguridad de los datos[25].

Mucho puede ser discutido sobre la idoneidad de los posibles sistemas a adoptar, ya que no es tarea fácil encontrar uno que reúna todos los requerimientos; así, el sistema de registro a través de contraseñas puede presentar una serie de inconvenientes[26] por tratarse de datos que se dejan a la memoria de la persona que los utiliza, que además debe ser instruida en la necesidad de preservar sus claves, no compartiéndolas con otros profesionales y asegurando el cierre de la sesión cada vez que deje de utilizar el equipo informático[27], especialmente si se encuentra en un área de uso común o a la que otros trabajadores pueden acceder[28] (toda vez que lo contrario puede permitir el acceso de otro profesional a datos de pacientes del profesional registrado, o bien el acceso por parte de un tercero a datos para los que quien está registrado no tiene autorización, con el consiguiente problema de identificación del verdadero infractor). Y, sin embargo, yéndonos al extremo opuesto, el uso de otros sistemas ciertamente más seguros, como la identificación a través del iris, la córnea, la huella dactilar u otros datos biométricos puede tener otras implicaciones en relación a los derechos de los propios profesionales, además de suponer un coste económico superior para su implementación y poder prestarse más a fallos mecánicos.

Un sistema utilizado ya en la práctica y que puede, tal vez, tomarse como referencia, es el del gallego IANUS, que supone la entrega de una tarjeta sanitaria a cada facultativo dotada con un chip que lleva incorporado un certificado digital, además de disponer la posibilidad de firma electrónica en toda la documentación clínica[29], si bien tampoco en este caso puede dejarse de incidir en la necesidad de concienciar al personal sanitario en materia de confidencialidad, en relación, en este caso, con el concreto aspecto del uso adecuado de sus claves, como medida complementaria pero necesaria. En este sentido, el propio Informe del Consello de Bioética sobre historia clínica reflexiona, tras la práctica supuesta por la entrada en vigor del sistema IANUS, que, si para proporcionar las "máximas garantías asistenciales" no se limita, de entrada,

[25] Puede verse, sobre esta cuestión, SAQUERO RODRÍGUEZ A., DE LA TORRE, I., DURANGO PASCUAL, A., "Análisis de aspectos de interés sobre privacidad y seguridad en la historia clínica electrónica", RevistaeSalud.com, vol. 7, nº 27, 2011.

[26] De ello nos advierte PINEDO GARCÍA, I., "Protección de datos sanitarios: la historia clínica y sus accesos", Revista CESCO de Derecho de Consumo, nº 8, 2013, pp. 311, 312.

[27] Es interesante, a estos efectos, el "Documento de seguridad del fichero de datos personales" preparado por el Servicio Madrileño de Salud, que, según la SAP Madrid (Sección 5ª), nº 78/2018, de 16 de octubre, da indicaciones expresas sobre el deber para los trabajadores de dejar su ordenador en estado tal que impida la visualización de datos protegidos cuando dicho trabajador abandone, de manera temporal o por haber finalizado su turno, su puesto de trabajo.

[28] Esta problemática se ha trasladado a algunas sentencias, como la SAP Madrid (Sección 16ª), nº 193/2018, de 13 de marzo, en la que se absuelve a dos enfermeras acusadas de acceder ilegítimamente a la historia clínica de la denunciante precisamente, entre otras causas, por no poderse acreditar que quienes efectivamente realizaron el acceso hubieran sido las personas denunciadas. Dice el Tribunal que de las pruebas testificales se desprende que es una práctica habitual –al menos, en el caso concreto que trata- "dejar los ordenadores abiertos cuando se consulta una historia clínica, de modo que otra persona puede venir después y aprovechando que la historia está abierta, consultarla", indicando también que "la mera huella informática o digital que refleja una consulta de un profesional en una historia clínica acredita que se ha entrado con las claves de dicho profesional, pero no que dicho profesional sea precisamente quien accede", con la relevancia que este extremo tiene en cuanto a la destrucción de la presunción de inocencia en el ámbito penal. Por el contrario, la reciente STS (Sala 2ª), nº 497/2018, de 23 de octubre, entiende que la posibilidad de que otra persona hubiera accedido a los datos valiéndose de las claves de las personas acusadas, a la vista de la actividad probatoria desplegada por las partes en el caso concreto, es una "mera posibilidad teórica" no acreditada.

[29] SÁNCHEZ CARO, J, "La historia…", cit., p. 78.

el acceso a estos datos (sin implicar un acceso indiscriminado[30]), esta posibilidad de acceso tan amplia otorgada por un sistema de historia clínica electrónica debe complementarse con exigencias de tipo *ético*[31].

No en vano, puede discutirse si el protocolo de acceso eficaz a estos efectos habría de ser, necesariamente, un sistema más restrictivo, toda vez que esto puede poner en peligro la salud de los pacientes. Resulta de especial interés la previsión que realiza el Grupo de Trabajo del artículo 29 en su *Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME)*, de 15 de febrero de 2007, o Documento WP131 (en adelante, documento WP131), en el que indica que el acceso por parte de personas no autorizadas debe ser virtualmente imposible si se quiere que el sistema sea aceptable desde el punto de vista de la protección de datos, mientras que el acceso de los profesionales autorizados en caso de necesidad real deberá ser prácticamente ilimitado para que el sistema cumpla con su propia finalidad para con los pacientes[32].

En suma, se trata de obtener un sistema eficaz y seguro capaz de alcanzar un (complicado) equilibrio entre la máxima seguridad de los datos y la accesibilidad a los mismos.

### III.2.2 *Módulos de acceso a los datos según tipos de datos y según la categoría profesional de quien accede.*

Otro de los mecanismos destinados a asegurar una mayor protección de los datos de salud contenidos en la historia clínica es el de los módulos de acceso, que permiten impedir o posibilitar el acceso a los datos de la historia clínica (o a algunos de ellos) según diversos criterios.

Precisamente en función del criterio utilizado pueden apreciarse dos categorías de módulos de acceso, que pueden darse conjuntamente o por separado en un mismo sistema: por una parte, aquéllos que permiten o no el acceso a datos concretos según el tipo de datos de que se trate; y, por otra, aquellos que se basan en la categoría profesional de quien trata de efectuar el acceso y la vinculación asistencial con el paciente que de la misma se deriva para autorizarlo o no a realizar dicho acceso o a acceder a un rango más o menos amplio de datos.

En cualquier caso, en relación a los módulos de custodia en general ha sido advertida la poca conveniencia de implantar un sistema excesivamente rígido, toda vez que podría ponerse en juego la salud del paciente al no tener acceso el profesional (que es, al fin y al cabo, la persona que, basándose en sus conocimientos especializados y experiencia profesional, ha de determinar qué datos puedan ser relevantes) a datos que pudieran tener alguna incidencia sobre

[30] No podemos olvidar que los principios de vinculación asistencial y de proporcionalidad siguen, en todo caso, vigentes, y que este mismo sistema prevé, entre otras cuestiones, el acceso a la información según distintos módulos de datos.

[31] Dice el informe que se ha de formular un "imperativo ético", es decir, que "no todo lo técnicamente posible es éticamente correcto o está permitido". En suma, se refiere a ese deber de confidencialidad (también nombrado expresamente en el Informe) y respeto de la legislación de protección de datos en los que estamos haciendo hincapié a lo largo del presente trabajo.

[32] P. 19 del documento.

Algo que puede destacarse de este mismo documento es que no sólo hace hincapié, en varias partes del mismo (pp. 15, 19, y otras), en la necesidad de adoptar protocolos seguros para el acceso a los datos por parte del personal sanitario, sino que también comenta la necesidad, en ocasiones obviada, de contar con sistemas que permitan identificar fidedignamente al paciente, puesto que lo contrario podría igualmente tener resultados perniciosos para los derechos de los pacientes a cuyos datos se tuviera acceso indebidamente por parte del personal sanitario o, también, por parte del particular que accede a los datos de un tercero como si fueran propios (pp. 14, 15).

el diagnóstico o el tratamiento, máxime si se tiene en cuenta la variada casuística que puede presentarse en la práctica[33].

Por esta razón, la cuestión de los módulos de acceso, en uno y otro caso, no ha estado exenta de debate, por lo que es conveniente estudiarla con mayor detenimiento.

### III.2.2.1 *El acceso a datos de salud especialmente sensibles. Los módulos de especial custodia.*

Si la generalidad de los datos de salud es de carácter sensible, existen algunos, como datos sobre enfermedades infecciosas, salud sexual, violencia de género, salud psiquiátrica, genética, y otros, que se consideran de una especial vulnerabilidad. Es por ello que se ha apuntado[34] que debe darse al paciente la posibilidad de ocultar la presencia de dichos datos en su historia clínica general, estableciéndose un sistema de "sobre cerrado", que consiste en consignar estos datos más vulnerables en módulos que se encuentran total o parcialmente ocultos, y a los que no se puede acceder salvo previa petición de acceso específica para esos datos, que puede concederse o no[35].

Se trata de un sistema más respetuoso con la intimidad de los pacientes, que, no obstante, es objeto de un importante debate, y es que se ha señalado que, de aparecer información sobre la existencia de dicho módulo de datos sensibles, el derecho a la intimidad y a la protección de los datos del paciente podría verse ya vulnerado[36]; posición que confronta con aquélla que defiende que, de no incorporarse un aviso sobre la existencia de dichos datos (aunque no se muestren éstos directamente), se podría estar privando al profesional de información necesaria a la hora de tratar con el enfermo, teniendo en cuenta, al fin y al cabo, que es el facultativo quien mejor puede conocer la implicación que estos datos pueden tener sobre la salud del paciente. Esta última posición nos parece la más razonable y ha sido secundada, también, por la doctrina[37] y por la propia AEPD, que en su Informe 656/2008 indica que este tipo de limitaciones de acceso al contenido pueden ir en perjuicio de la salud del paciente.

Ésta es, asimismo, la solución tomada por el gallego IANUS, el cual, entre otras innovaciones, ha adoptado el sistema de consignación de información en distintos módulos[38]

[33] SÁNCHEZ CARO, J., "La historia…", cit., pp. 71, 72.

[34] Documento WP131, de 15 de febrero de 2007, del Grupo de Trabajo del Artículo 29 (p. 14), Informe SESPAS (pp. 53, 54), SÁNCHEZ CARO, J. ("La historia…", cit., p. 70), y otros.

[35] En la propuesta del Informe SESPAS se indica, además, la necesidad de dejar constancia de dicho intento de acceso a efectos de posterior auditoría.

[36] El Grupo de Trabajo del Artículo 29 (en su documento WP131) pone la cuestión sobre la mesa, indicando que debería considerarse si es más adecuado enmascarar completamente la existencia de dicha información bloqueada (o completamente eliminada de la historia clínica), o bien dar algún tipo de aviso al respecto. Parece que el trabajo del Grupo apunta en una dirección proclive a conceder al paciente un amplio grado de autonomía en cuanto a sus propios datos, planteando opciones que van desde la posibilidad de eliminar algunos datos de la historia clínica (p. 15) hasta la posible conveniencia de que los pacientes decidan no participar en absoluto en el sistema de historia clínica electrónica y retirar sus datos de la misma, pasando por contemplar que la autorización para la consulta por el facultativo de los datos incluidos en el sistema de "sobre cerrado" que comentamos pueda ser otorgada únicamente por el propio paciente, y no por ninguna otra entidad o persona encargada (p. 14).

[37] Informe SESPAS (p. 54), SÁNCHEZ CARO, J. ("La historia…", cit., p. 70), ETREROS HUERTA, J. J. ("Historia…", cit., p. 190).

[38] En opinión de SÁNCHEZ CARO, la lista de supuestos sobre los que se podría aplicar esta previsión no puede considerarse taxativa ("La historia… cit.", p. 82).

que denomina "módulos de especial custodia" (art. 16), cuya existencia sí se prevé que sea advertida al facultativo (art. 17).

Por otra parte, en general, y no solamente en referencia a aquellos datos que revistan especial sensibilidad, se ha planteado que, en virtud del principio de proporcionalidad, el profesional debería acceder únicamente a los datos mínimos necesarios para prestar la asistencia sanitaria, sugiriéndose la idoneidad de separar la información contenida en la historia clínica en diversos módulos, con el fin de que el profesional pueda diferenciar los datos contenidos en la misma según diversos parámetros y así acceder únicamente a aquellos datos necesarios para la prestación de la asistencia concreta[39].

### III.2.2.2 *El acceso a la historia clínica basado en roles o perfiles profesionales.*

Se ha comentado también que la aplicación de los principios de proporcionalidad y, en particular, el de vinculación asistencial[40], podía aconsejar el establecimiento de módulos de acceso dependientes no del tipo de dato a consultar, sino de la categoría profesional de quien efectuara el acceso, de manera que se limitara el acceso para determinados tipos de perfiles[41] (aunque la cuestión podría no estar exenta de complicaciones prácticas[42]).

Es el caso, en primer lugar, de aquellos supuestos en los que es dudoso si la relación asistencial es de entidad suficiente como para legitimar un acceso (al menos, completo) a la historia clínica en virtud de la categoría profesional de quien dispensa la asistencia. Así, por ejemplo, los estudiantes de medicina en prácticas, residentes[43], los enfermeros[44], y otros

[39] Algo que puede ser de especial aplicación, por ejemplo, cuando el facultativo deba realizar una exploración o prueba muy concreta, o, también, en el caso de los enfermeros, debiendo distinguir asimismo en función de dónde presten sus servicios (Urgencias, planta, etc.), como indica RAMÍREZ NEILA, N., "Accesos legítimos a las historias clínicas electrónicas", en El derecho a la protección de datos en la historia clínica y la receta electrónica, Cáliz Cáliz, R., et al. (coord.), Thomson Reuters-Aranzadi, Cizur Menor, 2009, p. 294.

[40] Cabe apuntar, por cierto, que el artículo 8 de la norma gallega relaciona el acceso expresamente con la "asistencia directa", como bien destaca SÁNCHEZ CARO ("La historia…", cit., p. 79).

[41] Así lo hace el Grupo de Trabajo del Artículo 29 en su documento de 15 de febrero de 2007, recién citado, en el que remarca la necesidad de resolver la cuestión relativa a qué categorías de profesionales sanitarios pueden acceder a la historia clínica, además de proteger de mejor forma el derecho de los pacientes estableciendo un acceso a través de módulos basados en las distintas categorías profesionales (p. 15).

[42] Véase SAQUERO RODRÍGUEZ A., DE LA TORRE, I., DURANGO PASCUAL, A., "Análisis…", cit., p. 3.

[43] El *Protocolo mediante el que se determinan pautas básicas destinadas a asegurar y proteger el derecho a la intimidad del paciente por los alumnos y residentes en ciencias de la salud*, redactado por la Comisión de Recursos Humanos del Sistema Nacional de Salud y publicado por el Ministerio de Sanidad, Política Social e Igualdad en 2016, distingue entre los residentes, que pueden tener acceso a la historia clínica de los pacientes en cuanto que son, claramente, personal asistencial, y los alumnos de las titulaciones de Ciencias de la Salud, para los que la limitación de acceso al historial clínico es casi total, por considerar que su participación es más bien formativa, en lugar de asistencial.

[44] RAMÍREZ NEILA cree que no tendrían por qué acceder a la historia clínica completa ("Accesos…", cit., p. 294). El Informe 656/2008 de la AEPD se pronunció al respecto, indicando que los enfermeros podrán acceder, como mínimo, a la información relativa a la hospitalización concreta y a aquélla anterior que se considere relevante para la adecuada asistencia.
Con posterioridad, la STSJ de Castilla y León, Valladolid (Sala de lo Contencioso-Administrativo, Sección 1ª), nº 206/2018, de 28 de febrero, trata esta precisa cuestión. En este caso, la sentencia recurrida estimaba que el programa informático al que accedía el personal de enfermería era adecuado para la realización de las funciones propias de este grupo profesional, estimándose que éstas no precisan la consulta completa del historial clínico; algo que discute la parte recurrente. Analizando la legislación aplicable –entre otras, la Ley de Ordenación de las Profesiones Sanitarias-, el Tribunal sentenciador indica que será preciso analizar las funciones propias de cada categoría profesional con el fin de conocer si para su ejercicio se precisará el acceso a la historia clínica o no, concluyendo que, en el caso de los enfermeros, las actividades propias de su actividad exigen el acceso a dichos datos; acceso que el programa utilizado

profesionales del ámbito sanitario. Será preciso estar a lo dispuesto por la Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias, que realiza una distinción entre lo que considera "profesiones sanitarias reguladas" y "profesionales del área sanitaria de formación profesional", considerando que los profesionales del primer tipo ostentarían el derecho de acceso a la historia clínica, y no así los del segundo[45]; también al régimen específico de cada una de estas profesiones; y, en fin, a la idea de la limitación de acceso según la concreta vinculación asistencial del profesional con el paciente, en general[46].

Más problemáticos pueden parecer los accesos efectuados por profesionales no ligados al paciente por vinculación asistencial alguna: así, los realizados por el personal de administración y gestión. No obstante, artículo 16.4 LAP da una solución muy clara, y es que éstos sólo podrán tener acceso a los datos relacionados con sus propias funciones[47]; algo que podría aplicarse, según algunas opiniones[48], a profesionales que no tuvieran tampoco vinculación asistencial con el paciente, como los trabajadores sociales[49].

En cualquier caso, es importante reseñar aquí la previsión de reserva sobre los datos clínicos que el artículo 2.7 LAP extiende sobre toda persona que tenga acceso a los mismos, así como tener en cuenta lo que parece ser una tendencia a interpretar las posibilidades de acceso de manera restrictiva[50].

### III.2.3 *Bloqueo de determinados datos respecto de profesionales concretos perfiles profesionales.*

Se trata de una solución sin vocación de generalidad, que puede preverse para casos muy específicos en los que se dé una circunstancia que requiera de una especial protección, y que habría de permitir, desde el punto de vista técnico, el bloqueo de datos (de cualquier tipo, incluso aquéllos en principio menos comprometidos, como el teléfono o la dirección[51]) respecto de un profesional en concreto; por ejemplo, cuando existieran antecedentes de violencia de género.

---

no garantizaba. Por el contrario, El TSJ analiza –en la misma sentencia- la situación de los Técnicos en Cuidados Auxiliares de Enfermería para determinar que, en este caso, el acceso no estaría justificado por sus actividades.

[45] No obstante, parece que cada vez hay más problemas para efectuar la distinción de manera inequívoca en la práctica, siendo creciente el número de supuestos en el que profesionales que, en principio, es dudoso que tengan vinculación asistencial con el paciente, solicitan acceder a los datos contenidos en la historia clínica (*vid.* GONZÁLEZ GARCÍA, L., "Derecho…", cit., pp. 277, 278).

[46] Aspecto en el que incide RAMÍREZ NEILA ("Accesos…", cit., p. 294).

[47] *Vid*., también, el Informe 0248/2005 de la AEPD. Por otra parte, ésta es la solución aportada por varios ejemplos de la legislación autonómica (véase (GONZÁLEZ GARCÍA, L., "Derecho…", cit., pp. 277, 278).

[48] Para RAMÍREZ NEILA, deberá mediar el consentimiento expreso del paciente para el acceso a los datos que no estén relacionados con las funciones propias de éstos ("Accesos…", cit., p. 296). Una opinión similar se encuentra en TRONCOSO REIGADA, A., "La confidencialidad…", cit., pp. 103, 104.

[49] Ésta es la solución tomada en el Decreto 29/2009 gallego tras la modificación efectuada en virtud del Decreto 164/2013, que introduce la figura del trabajador social junto con la del personal de gestión y servicios en el artículo 9, que indica que el personal perteneciente a estos grupos sólo podrá acceder a los datos imprescindibles para el ejercicio de las funciones propias de su puesto de trabajo, añadiéndose que los trabajadores sociales únicamente podrán acceder a los apartados correspondientes a aspectos sociales y sociosanitarios de la historia clínica.

[50] *Vid.*, en general, las obras de RAMÍREZ NEILA y GONZÁLEZ GARCÍA citadas en las notas al pie precedentes.

[51] Y es que datos *mínimos* pueden ser sensibles en según qué circunstancias, razón por la cual se ha de mantener una necesaria flexibilidad en la concepción de los datos que pueden o no ser compartidos (GERVÁS, J, "Historia clínica: al limitar el acceso se mejora el proceso", Actualización en Medicina de Familia, vol. 11, nº 7, 2015, pp. 312, 373 (8, 9). En línea: http://amf-semfyc.com/web/article_ver.php?id=1448).

Podría encontrarse apoyo a esta solución aquí propuesta en el Informe 0054/2010 de la AEPD, que apunta a la posibilidad del paciente de excluir la posibilidad de acceso a los datos de su historia clínica a profesionales concretos (si bien lo hace al resolver una consulta relacionada con un sistema concreto de almacenamiento de los datos clínicos).

### III.2.4 *Implantación de un sistema informático capaz de detectar accesos indebidos y de efectuar notificaciones al responsable de los datos.*

Como complemento a un protocolo de acceso que sea suficientemente seguro, puede ser también útil disponer de *software* que, yendo un paso más allá del registro de accesos que después se tratará, sea capaz no sólo de almacenar toda la información relativa a éstos, sino también de detectar cuándo se están llevando a cabo accesos potencialmente no justificados[52] y generar una notificación o alarma que pueda evitar que el acceso ilegítimo continúe o se repita en el futuro por parte del mismo u otros usuarios.

Ésta es la idea situada tras el sistema de plataforma centralizada de *logs* (accesos) implantado en el Ib-Salut (el servicio de salud de las Islas Baleares), el cual persigue una identificación y detección proactiva de accesos potencialmente indebidos, localizando aquéllos que no se ajusten, en principio, a un uso correcto de los sistemas, como pueden ser los supuestos de acceso masivo a la historia clínica de un paciente por distintos profesionales, el acceso por personal no asistencial, y otros, y que cuenta con un sistema de generación de alarmas a tiempo real de accesos injustificados[53].

### III.3 *Registros de accesos.*

Se preveía en el artículo 103 del Reglamento de desarrollo de la LOPD, y también, de modo general, en el artículo 23 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ya lo he nombrado antes, ver cómo lo nombro aquí) en el ámbito de la Administración Electrónica, previendo el primero de los citados, más específico, que de cada intento de acceso quedarían registrados, como mínimo, la identificación del usuario, la fecha y hora del acceso, el fichero accedido, el tipo de acceso, y si éste ha sido denegado o autorizado, debiendo conservarse esta información durante al menos dos años.

La AEPD ha interpretado este artículo en el sentido de que lo esencial es contar con la información que permita identificar inequívocamente a la persona que realice el acceso y a qué información concreta accedió (Informe 584/2009).

Se trata de una medida de control interno totalmente necesaria[54] para la detección de accesos indebidos, y que es clave para la persecución de los mismos a través de la realización

[52] Obsérvese que hablamos de accesos *potencialmente* injustificados: siempre habrá de tenerse en cuenta que la valoración de si el acceso ha sido o no justificado no corresponderá en ningún caso al *software*, sino a la persona competente).

[53] *Vid.* BENITO TOVAR, M. A. y ÁLVAREZ SALAZAR, E., "Plataforma centralizada de logs del Ib-Salut", Revista de la Sociedad Española de Informática y Salud, nº 122, 2017, p. 18.

[54] Según indicaba el artículo 103 del Reglamento de desarrollo de la LOPD, existiría un único caso en el que podría prescindirse de este registro de accesos: cuando el responsable del fichero sea una persona física que garantice que es la única que tiene acceso a los datos; en particular, en el caso de los médicos con consulta privada. En este sentido se pronuncia, también, el Informe SESPAS (p. 65). Se trataría, en todo caso, de una excepción (y, aun así, cabe imaginar que el paciente del médico particular pueda no querer que éste se dedique a entrar de forma indiscriminada y sin razón aparente a sus datos de salud).

controles o auditorías por parte de la propia Administración, de empresas encargadas, o de los propios interesados. Por ello, parece probable su mantenimiento (o el de algún sistema muy similar) tras la entrada en vigor de la nueva LOPDGDD.

### III.4 *Auditorías por parte de la propia Administración o por parte de empresas externas*.

El ejercicio de auditorías sobre la actividad de la Administración en relación con la protección de datos ha sido propuesto ya por diversas fuentes, entre ellas, el Informe SESPAS[55] y el Grupo de Trabajo del Artículo 29[56], y es que parece ciertamente necesario someter la actuación de la Administración y sus trabajadores a un control que permita determinar si ésta se lleva a cabo con total respeto por la legislación vigente, posibilitando, en su caso, la detección de comportamientos contrarios a las normas y la depuración de las responsabilidades que correspondan.

Este tipo de auditorías puede darse por parte de la propia Administración, que puede efectuar un control en materia de datos sobre sus propios organismos, o por parte de empresas externas a la Administración a las que se encarguen estos servicios.

Como puede imaginarse, para efectuar estos controles es imprescindible que quede constancia de los accesos efectuados, con todos los detalles preceptivos para la identificación del tipo de acceso y del individuo que lo llevó a cabo, lo cual sólo puede darse a través del anteriormente mentado registro de accesos.

Por otra parte, el artículo 54 LOPDGDD se refiere también a la realización de auditorías aunque en un sentido ligeramente distinto, al disponer que la Presidencia de la AEPD podrá realizar auditorías preventivas referidas a un sector concreto de actividad, de las cuales podrán resultar directrices que serán de obligado cumplimiento para el sector o responsable al que la auditoria se refiera; lo cual es manifestación de la previsión realizada por el artículo 58 RGDP que reconoce, entre los poderes de investigación conferidos a la autoridad de control, el de realizar estas auditorías de protección de datos.

### III.5 *Control por parte de los afectados.*

El control por parte de los afectados de sus propios datos es, como puede imaginarse, de vital importancia[57]. En relación con la historia clínica y los accesos no justificados, en particular, este control requiere que se articulen los mecanismos adecuados para asegurar el derecho a la trazabilidad de los propios datos, la cual debería permitir conocer, entre otras cuestiones, si se ha dado un acceso ilegítimo a los datos (independientemente del hecho de que no son pocas las veces que éste llega a su conocimiento, precisamente, por haberse transmitido los datos a terceros), así como el tratamiento que, en general, se da a sus datos, en el marco del ejercicio de los derechos que tanto el Reglamento (en su Capítulo III) como la LOPDGDD (en su Título III) les reconocen.

[55] P. 51 Informe SESPAS.

[56] Documento WP131, p. 21.

[57] El Proyecto de Historia Clínica Digital en el Sistema Nacional de Salud del Ministerio de Sanidad, proyecto que persigue la interoperabilidad de las historias clínicas almacenadas en los distintos Servicios de Salud de las Comunidades Autónomas, se refiere al control por parte de los ciudadanos al nombrarles como "auditores externos del sistema" y reconocerles el acceso a (sólo) algunos de los datos del registro de accesos (p. 16).

Precisamente, la trazabilidad de los propios datos se ha entendido comprendida en el derecho de acceso que hasta fechas recientes se encontraba regulado en el artículo 15.1 LOPD (y también, de manera más específica, en el artículo 18 LAP), ahora recogido en los artículos 13 LOPDGDD y 15 RGDP, y en el cual se ha considerado incluido el derecho a acceder al registro de accesos anteriormente comentado.

Ahora bien, la completa trazabilidad de los datos se ha visto limitada por una cortapisa importante, y es que en más de una ocasión se ha considerado que el dato de la identidad de quien efectúa el acceso a los datos no está comprendido en esa trazabilidad que se entiende incluida en el derecho de acceso[58]. Aunque no podemos extendernos en esta cuestión, que realmente presenta mayor complejidad que la que se pueda desarrollar aquí, se ha de decir que existen, como mínimo, dudas razonables respecto a las razones que amparan la decisión de no comunicar esta información al interesado.

Además del acceso por parte del interesado al registro de accesos (o el mecanismo que, en su caso, lo sustituya), podrían existir otras vías para el mismo de obtener información sobre sus datos (en este caso, sobre su seguridad), como la que se presenta a razón de la obligación para el responsable del tratamiento de notificar la *brecha de seguridad* sufrida por la seguridad de los datos, en algunos casos[59], al propio interesado (art. 34 RGPD), si bien nos situaríamos en este escenario únicamente cuando ya se hubiera dado un acceso ilegítimo detectado por el sistema de seguridad dispuesto para la protección de los datos.

No obstante, ha de tenerse en cuenta que no en todos los supuestos en los que un tercero accede a los datos habría una violación del sistema de seguridad o sería ésta detectable como tal: así sucedería, por ejemplo, cuando se utilizaran las claves de un compañero para acceder al historial clínico de un paciente al que éste trata, o cuando la sesión de un médico se dejara abierta en un ordenador de uso común o situado en una zona de libre acceso. O incluso, por pensar en otros posibles supuestos, cuando un profesional consultara una historia clínica en presencia y a la vista de otro.

En todo caso, el control por parte de los afectados tiene relevancia no sólo como control a posteriori de las violaciones del sistema de seguridad de los datos, sino también como medida preventiva, por el positivo efecto disuasorio que pueda tener sobre las malas prácticas en esta materia, y como parte de los derechos de los interesados, de modo que puedan conocer cuál es el tratamiento exacto que se está dando a sus datos en todo momento.

## IV. CONCLUSIONES

La seguridad de los datos de salud contenidos en la historia clínica es uno de los muchos retos que todavía hoy se mantienen en materia de derecho de protección de datos. Y es que, si bien se trata de un ámbito en el que se han producido notables avances durante los últimos años (véase, por ejemplo, el sistema IANUS de acceso a la historia clínica de Galicia), los datos que arroja la práctica demuestran que el acceso indebido a la historia clínica por parte del personal sanitario sin vinculación asistencial –que es la cuestión que nos ocupa- sigue siendo una constante en nuestro sistema sanitario, y ello incluso en las áreas que poseen

[58] Ésta es la posición de la propia AEPD (Informes 167/2005 y 171/2008, entre otros).

[59] El art. 34.1 RGPD dispone el deber de efectuar dicho aviso al interesado sólo cuando sea "probable" que dicha violación "entrañe un alto riesgo para los derechos y las libertades de las personas físicas", por lo que habría que estudiar su aplicabilidad al supuesto que nos ocupa.

sistemas de protección de los datos más avanzados, como es el caso del mentado sistema gallego.

Mantener la seguridad de los datos contenidos en la historia clínica es una tarea compleja[60]. Por una parte, la historia clínica es un instrumento de total necesidad para la prestación de la correcta asistencia sanitaria. Gracias a ella, los profesionales pueden conocer los antecedentes clínicos del paciente al que tratan, así como los diagnósticos y tratamientos a los que se encuentre sometido, emitidos por profesionales de cualquier centro sanitario y cualquier especialidad médica, como indica el propio artículo 14.1 LAP. Es, así, un conjunto de datos de uso imprescindible para el personal sanitario, que incluso llega a configurarse como un deber para los mismos.

Sin embargo, por otro lado, es también indispensable asegurar la confidencialidad de los datos como principio básico de la relación médico-paciente, resultando así que su ruptura puede acarrear consecuencias perniciosas varias. Y es que no sólo se causa un perjuicio al paciente que ve sus derechos conculcados, sino que también la propia entidad en el seno de la cual se produce la violación de derechos se verá afectada negativamente. Esto se ve de manera muy clara respecto de la sanidad privada, en la que la falta de confianza puede tener una consecuencia económica directa más apreciable[61], pero también puede predicarse respecto de la sanidad pública, ámbito en el que la repercusión se traslada, incluso, al total de la sociedad, en la medida en que la pérdida de confianza de los ciudadanos en el sistema sanitario estatal puede determinar que muchos de ellos dejen de tratarse, con las evidentes consecuencias en materia de salud pública (cuestión sobre la que ya ha advertido el Tribunal Europeo de Derechos Humanos[62]).

Como se ve, en esta materia nos movemos siempre en un terreno en el que la tensión entre la salud y la intimidad de los pacientes condiciona cualquier posible medida a adoptar[63]; tensión que se acentúa todavía más con la adopción de sistemas de historia clínica electrónica que, si bien suponen grandes ventajas, pueden implicar también un mayor peligro en orden a la

[60] En este sentido, es conveniente recordar la precisión que realizaba el Grupo de Trabajo del artículo 29 respecto a la necesidad de disponer de un sistema que impida por completo el acceso a personas no autorizadas pero que al mismo tiempo garantice el acceso pleno a los profesionales autorizados para que el sistema cumpla con su propia finalidad para con los pacientes (Documento WP131, p. 19).

[61] VALDUNCIEL subraya que las fallas de seguridad en el sistema de protección de los datos personales de los clientes de cualquier empresa puede dañar, directa o indirectamente, la actividad económica de la misma, provocando pérdida de reputación, de clientes, etc. (VALDUNCIEL, V., "La aplicación del Reglamento General de Protección de Datos en el Sector Salud de Datos", Revista de la Sociedad Española de Informática y Salud, nº 122, 2017, p. 15).

[62] El Tribunal Europeo de Derechos Humanos ha hecho hincapié en diversas ocasiones en la importancia del mantenimiento del carácter confidencial de los datos de salud como mecanismo para preservar la confianza de los ciudadanos en los servicios de salud, cuestión de capital importancia tanto para los pacientes individualmente considerados, como para la comunidad al completo, por el efecto que pudiera tener, por ejemplo, una enfermedad infecciosa que no recibiera tratamiento por falta de confianza del enfermo en el sistema sanitario (*vid.* DE LA SERNA BILBAO, M. N. y FONSECA FERRANDIS, F., "El acceso a la historia clínica; el alcance del derecho", en Los retos del Estado y la Administración del siglo XXI: libro homenaje al profesor Tomás de la Quadra-Salcedo Fernández del Castillo, vol. 2, tomo 2, Parejo Alfonso, L. J. (coord.), y Vida Fernández, J. (coord.), Madrid, 2017, p. 2285).

En el mismo sentido, otros autores como ORDÁS ALONSO, que incide en que el secreto médico no se encuentra establecido tan sólo en interés del paciente, sino que también hay un interés público en preservar la confianza de los ciudadanos en el sistema sanitario ("Intimidad…", cit., pp. 784, 785 y 792, 793), o TRONCOSO REIGADA, para quien la confidencialidad es "un bien constitucional colectivo" ("La confidencialidad…", cit., pp. 48, 49).

[63] Para TRONCOSO REIGADA, en esta materia hay una colisión entre el derecho a la vida que conlleva la atención sanitaria (la cual requiere acceder a los datos de salud de las personas), y el derecho a la intimidad, representado por la confidencialidad que precisa esta información. Para el autor, no se trataría de optar entre el derecho a la intimidad y una atención sanitaria eficaz, sino de buscar el respeto a todos ellos a través del principio de proporcionalidad ("La confidencialidad…", cit., p. 49).

confidencialidad de los datos de salud de los pacientes, por el gran número de personas que pueden llegar a entrar en contacto con los mismos.

Como se ha dicho, a lo largo de las últimas décadas se han propuesto varios mecanismos para remediar los accesos injustificados, entre los que destaca el ya muchas veces mencionado y pionero sistema IANUS de la sanidad gallega, a pesar de lo cual los accesos indebidos se han seguido produciendo, como se desprende de las estadísticas que maneja, por ejemplo, el Consello de Bioética de Galicia (antes reseñadas), o algunas de las sentencias condenatorias referenciadas a lo largo del trabajo.

Pero, además de que la incidencia práctica de los accesos indebidos por parte del personal sanitario reclame una revisión de los mecanismos de prevención de dichos accesos, la reciente aprobación de la nueva legislación de protección de datos (RGPD y LOPDGDD) abre un nuevo escenario en materia de seguridad de los datos personales. El nuevo modelo, que parte de la responsabilidad proactiva de los sujetos responsables de los datos, así como de la necesidad de introducir medidas de seguridad desde el diseño y por defecto, requiere que para cada tratamiento se apliquen las medidas técnicas y organizativas de seguridad más adecuadas, a lo cual debe preceder un estudio de la actividad y del riesgo que para los datos personales de los interesados supone el tratamiento concreto.

Todo ello refuerza la necesidad de poner en marcha mecanismos capaces de asegurar la mayor protección de los datos, y, en el caso de la historia clínica, de replantear cuáles han de ser esos mecanismos concretos.

Precisamente en este sentido, y entendiendo que no existe solución única infalible, se han presentado una serie de medidas que, aplicadas en conjunto, se entiende que permitirían, al menos, mejorar los niveles de seguridad de los datos contenidos en las historias clínicas, al tiempo que seguirían garantizando el acceso al personal autorizado, manteniendo, así, ese delicado equilibrio entre seguridad de los datos y salud del paciente. Se trata, como se ha visto, de una serie de mecanismos que pasan por la formación en protección de datos y confidencialidad, la optimización de los medios técnicos en los sistemas de historia clínica electrónica empleados, o el debido control del tratamiento por parte de los sujetos involucrados.

Sin perjuicio, en fin, de que las propias características del sistema dificulten la eliminación absoluta de los accesos indebidos, y teniendo presente que por ello el sistema debe completarse, además, con aquellas consecuencias que se deriven del acceso injustificado (tema interesante y de importancia, pero que excede del objeto de nuestro trabajo), creemos que se ha de realizar un esfuerzo, siguiendo los dictados y el espíritu de la nueva normativa de protección de datos, por procurar la seguridad de los datos desde la propia creación de los sistemas de historia clínica electrónica, al tiempo que se vela por la correcta formación de los profesionales que con ellos se relacionan.

Sólo así, aplicando todas estas medidas en conjunto, podrá avanzarse en la prevención de acceso indebido a la historia clínica por parte del personal sanitario sin vinculación asistencial.

## V. REFERENCIAS BIBLIOGRÁFICAS


- BARRAL, I., “Datos relativos a la salud e historia clínica: la confidencialidad de los datos médicos”, en Protección de datos personales en la sociedad de la información y la

vigilancia, Llácer Matacás, M. R. (coord.), *La Ley*, Madrid, (2011), pp. 352-368.

- BENITO TOVAR, M. A. Y ÁLVAREZ SALAZAR, E.: "Plataforma centralizada de logs del Ib-Salut", *Revista de la Sociedad Española de Informática y Salud*, nº 122, (2017), pp. 18-21.
- DE LA SERNA BILBAO, M. N. Y FONSECA FERRANDIS, F., "El acceso a la historia clínica; el alcance del derecho", en Los retos del Estado y la Administración del siglo XXI: libro homenaje al profesor Tomás de la Quadra-Salcedo Fernández del Castillo, vol. 2, tomo 2, Parejo Alfonso, L. J. (coord.), y Vida Fernández, J. (coord.), Madrid, (2017), p. 2271-2320.
- ETRERos HUERTA, J. J., "Historia clínica electrónica", en El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica, Cáliz, R. (coord.), et al., Thomson Reuters-Aranzadi, Cizur Menor, (2009), pp. 181-200.
- GERVÁS, J., "Historia clínica: al limitar el acceso se mejora el proceso", Actualización en Medicina de Familia, vol. 11, nº 7, Barcelona, (2015), pp. 312, 373 (8, 9). En línea: http://amf-semfyc.com/web/article_ver.php?id=1448
- GÓMEZ PIQUERAS, C., La historia clínica. Aspectos conflictivos resueltos por la Agencia Española de Protección de Datos, en El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica, Cáliz, R. (coord.), et al., Thomson Reuters-Aranzadi, Cizur Menor, (2009), pp. 127-160.
- GONZÁLEZ GARCÍA, L., "Derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos", en *Derecho y Salud*, vol. 24, nº EXTRA-1, (2014), pp. 274-285.
- ORDÁS ALONSO, M., "Intimidad, secreto médico y protección de datos sanitarios", en Razonar sobre Derechos, García Amado, J. A. (coord.), Tirant lo Blanch, Valencia, (2016), pp. 773-834.
- PEREIRA ÁLVAREZ, M., "El tratamiento de los datos en las HCE y las medidas de seguridad: una aproximación desde el punto de vista técnico. Especial Referencia al nuevo Reglamento de desarrollo de la LOPD", en El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica, Cáliz Cáliz, R. (coord.), et al., Thomson Reuters-Aranzadi, Cizur Menor, (2009), pp. 305-320.
- PINEDO GARCÍA, I., "Protección de datos sanitarios: la historia clínica y sus accesos", en *Revista CESCO de Derecho de Consumo*, nº 8, (2013), pp. 306-318.
- RAMÍREZ NEILA, N., "Accesos legítimos a las historias clínicas electrónicas", en El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica, Cáliz Cáliz, R. (coord.), et al., Thomson Reuters-Aranzadi, Cizur Menor, (2009), pp. 289-304.
- SÁNCHEZ CARO, J., "La historia clínica gallega: un paso importante en la gestión del conocimiento", en *Derecho y salud*, vol. 18, nº 1, (2009), pp. 57-86.
- SAQUERO RODRÍGUEZ A., DE LA TORRE, I., DURANGO PASCUAL, A., "Análisis de aspectos de interés sobre privacidad y seguridad en la historia clínica electrónica", RevistaeSalud.com, vol. 7, nº 27, (2011).
- SERRANO PÉREZ, M. M., "Salud pública, epidemiología y protección de datos", en Tratado de Derecho Sanitario, vol. I, Larios Risco, D. (coord.), et al., Thomson Reuters-Aranzadi, Cizur Menor, 2013, pp. 1091-1113.
- TRONCOSO REIGADA, A., "La confidencialidad de la historia clínica", en *Cuadernos de Derecho Público*, nº 27, enero-abril (2006), pp. 45-143.
- VALDUNCIEL, V.: "La aplicación del Reglamento General de Protección de Datos en el Sector Salud de Datos", en *Revista de la Sociedad Española de Informática y Salud*, nº 122, 2017, pp. 15-17.

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: informes jurídicos 0248/2005, 167/2005, 656/2008, 171/2008, 584/2009 y 0054/2010.
- DECÁLOGO DE LA HISTORIA CLÍNICA ELABORADO POR LA COMISIÓN CENTRAL DE DEONTOLOGÍA DE LA ORGANIZACIÓN MÉDICA COLEGIAL DE ESPAÑA Y LA COMISIÓN PERMANENTE DEL CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS, 2017: http://www.comalmeria.es/sites/default/files/noticias/docs/decalogo_sobre_historia_clinica.pdf
- DOCUMENTO DE TRABAJO SOBRE EL TRATAMIENTO DE DATOS PERSONALES RELATIVOS A LA SALUD EN LOS HISTORIALES MÉDICOS ELECTRÓNICOS (HME) (DOCUMENTO WP131), DE 15 DE FEBRERO DE 2007, DEL GRUPO DE TRABAJO DEL ARTÍCULO 29: https://www.apda.ad/sites/default/files/2018-10/wp131_es.pdf
- DIRECTRICES SOBRE LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD) Y PARA DETERMINAR SI EL TRATAMIENTO "ENTRAÑA PROBABLEMENTE UN ALTO RIESGO" A EFECTOS DEL REGLAMENTO (UE) 2016/679 (DOCUMENTO WP248), EN LA VERSIÓN REVISADA DE 4 DE OCTUBRE DE 2017, DEL GRUPO DE TRABAJO DEL ARTÍCULO 29: https://www.aepd.es/media/criterios/wp248rev01-es.pdf
- ÉTICA EN EL ACCESO Y EN EL USO DE LA DOCUMENTACIÓN CLÍNICA: REFLEXIONES Y RECOMENDACIONES, CONSELLO DE BIOÉTICA DE GALICIA, 2017: https://extranet.sergas.es/catpb/Docs/cas/Publicaciones/Docs/AtEspecializada/PDF-2669-es.pdf
- PROTECCIÓN DE DATOS PERSONALES Y SECRETO PROFESIONAL EN EL ÁMBITO DE LA SALUD: UNA PROPUESTA NORMATIVA DE ADAPTACIÓN AL RGDP, PRESENTADO POR LA SOCIEDAD ESPAÑOLA DE SALUD PÚBLICA Y ADMINISTRACIÓN SANITARIA (SESPAS), 2017: http://sespas.es/2017/11/30/proteccion-de-datos-personales-y-secreto-profesional-en-el-ambito-de-la-salud-una-propuesta-normativa-de-adaptacion-al-rgpd/
- PROTOCOLO MEDIANTE EL QUE SE DETERMINAN PAUTAS BÁSICAS DESTINADAS A ASEGURAR Y PROTEGER EL DERECHO A LA INTIMIDAD DEL PACIENTE POR LOS ALUMNOS Y RESIDENTES EN CIENCIAS DE LA SALUD, COMISIÓN DE RECURSOS HUMANOS DEL SISTEMA NACIONAL DE SALUD, 2016: https://www.boe.es/buscar/doc.php?id=BOE-A-2017-1200
- PROYECTO DE HISTORIA CLÍNICA DIGITAL EN EL SISTEMA NACIONAL DE SALUD DEL MINISTERIO DE SANIDAD: http://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf