ene
revista de enfermería

EVOLUCIÓN HISTÓRICA DEL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS EN HOSPITALES PÚBLICOS DE ESPAÑA

HISTORICAL EVOLUTION OF COMPLIANCE WITH DATA PROTECTION REGULATIONS IN PUBLIC HOSPITALS OF SPAIN

Autores: Salud Ávalos Giménez, Nicolás Fernández García

Hospital General de La Palma. Servicio Canario de Salud

Universidad de La Laguna

Fernández García, N., & Avalos Gimenez, S. (2020). **EVOLUCIÓN HISTÓRICA DEL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS EN HOSPITALES PÚBLICOS DE ESPAÑA**. *Ene, 14*(1).
Consultado de http://ene-enfermeria.org/ojs/index.php/ENE/article/view/860

RECIBIDO: Septiembre 2018
ACEPTADO: Octubre 2019
PREEDICIÓN: Diciembre 2019
PUBLICADO: Abril 2020

Resumen

El derecho a la protección de los datos de salud es considerado un derecho fundamental en España, que goza por lo tanto de especial protección mediante normas nacionales, además de europeas. El objetivo de este trabajo es analizar el grado de cumplimiento de la normativa legal sobre protección de datos por parte de los hospitales públicos españoles, a lo largo de los últimos 25 años. El análisis bibliográfico realizado muestra un aumento gradual de la observancia del reglamento por parte de los profesionales y las instituciones, aunque de las distintas evaluaciones realizadas se deriva que todavía quedan aspectos por cumplir de unas normativas españolas y europeas que son cada vez más exigentes con este derecho fundamental.

Palabras clave: Confidencialidad; Datos de Salud Generados por el Paciente; Ética Institucional; Hospitales públicos; Seguridad del Paciente.

Abstract

The right to protection of health data is considered a fundamental right in Spain, which therefore enjoys special protection through national as well as European rules. The aim of this work is to analyse the degree of compliance with legal regulations on data protection by Spanish public hospitals over the last 25 years. The bibliographical analysis carried out shows a gradual increase in the observance of the regulations by professionals and institutions. However, the different evaluations carried out show that there are still aspects to be complied with in Spanish and European regulations which are increasingly demanding with this fundamental right.

Keywords: Confidentiality; Ethics, Institutional; Hospitals, public; Patient Generated Health Data; Patient Safety.

INTRODUCCIÓN

En España, el derecho a la protección de datos es considerado como un derecho fundamental que goza de especial protección. Así, en el artículo 18.1 de la Constitución española (1), se recoge que *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"*. En el 18.4 se especifica además 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"*.

A medida que aumenta la sensibilidad de los datos de una persona por pertenecer a una esfera más íntima de su vida, se aumenta el grado de protección en el tratamiento de este tipo de datos (2). Es por ello que dentro de los datos personales existen algunos especialmente protegidos que quedan regulados en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) (3). Los datos que esta ley recoge como de especial protección son los relacionados con:

- La ideología, afiliación sindical, religión y creencias.
- El origen racial, la salud y la vida sexual.
- La comisión de infracciones penales o administrativas.

La enfermedad pone a la persona en una posición de vulnerabilidad y es en ese momento de enfermedad cuando la persona revela a los profesionales sanitarios información sobre una esfera muy personal de su vida, con el ánimo de restablecer su salud. Por tanto, los profesionales sanitarios manejamos en nuestro ámbito laboral, cualitativa y cuantitativamente importantes datos personales. En la actualidad España tiene 799 hospitales, de los cuales 339 son públicos y 460 son de propiedad privada, según figura en el Catálogo Nacional de Hospitales 2018 del Ministerio de Sanidad, Servicios Sociales e Igualdad (4), lo que nos da una idea de la cantidad de datos que se producen en la atención hospitalaria.

Históricamente, cuando se producía una vulneración de los profesionales sanitarios del derecho a la protección de datos, ésta se originaba principalmente por dos motivos: por la ignorancia de dicho derecho fundamental y por un peligroso voluntarismo orientado a procurar una adecuada asistencia sanitaria a sus pacientes (5). Por lo tanto, la divulgación no consentida de datos personales podría acarrear problemas legales a los profesionales, además de tener posibles consecuencias para el paciente. Es por

ello por lo que resulta fundamental la comprensión por parte de los profesionales de la importancia de la protección de datos en su trabajo. En nuestro caso, como enfermeras, la confidencialidad y el secreto profesional asume un especial protagonismo en el Código Deontológico de la enfermería española, en cuyo articulado se establece entre otros aspectos que "la enfermera guardará en secreto toda la información sobre el paciente que haya llegado a su conocimiento en el ejercicio de su trabajo".(6)

Dado que el grado de cumplimiento en protección de datos se lleva monitorizando en los hospitales españoles desde hace varias décadas, creemos interesante recoger en este trabajo cómo se ha desarrollado su acatamiento durante este tiempo. Por ello, el objetivo general de este trabajo es analizar la evolución histórica del cumplimiento de la normativa de protección de datos en los hospitales públicos españoles.

Conceptos Clave

A lo largo de este artículo aparecen varios conceptos clave que es necesario que sean definidos ya que se utilizarán con bastante frecuencia, como son el concepto de d*ato personal, dato de salud, historia clínica, historia clínica electrónica, tratamiento de datos, responsable del fichero o tratamiento* y *encargado del tratamiento*. Estas definiciones se recogen fundamentalmente en la LOPD, del 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 (RLOPD) (7) y del nuevo Reglamento General de Protección de Datos (RGPD) europeo (8) que comenzó a aplicarse el 25 de mayo de 2018. También se recogen definiciones de conceptos recogidas en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (LAP) (9).

DATO PERSONAL

La LOPD define en su artículo 3 el *"dato de carácter personal"* como *"cualquier información concerniente a personas físicas identificadas o identificables"*. Ahora bien, ¿qué se entiende por persona identificable? De acuerdo con el RLOPD en su artículo 5 se considera *"persona identificable"* a *"toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha iden-*

tificación requiere plazos o actividades desproporcionados".

DATO DE SALUD O DATO RELATIVO A LA SALUD

El RLOPD en su artículo 5 define los datos relacionados con la salud como *"las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética"*.

La catedrática Yolanda Gómez Sánchez considera que el dato de salud es *"cualquier dato obtenido en el ámbito biomédico, ya responda estrictamente a un tratamiento médico o cualquier otra prestación que tenga que ver con su bienestar físico o psíquico, aunque la misma no responda a la necesidad de tratar una enfermedad en sentido estricto"* (10).

HISTORIA CLÍNICA

La LAP, en su artículo 3, recoge que la historia clínica (HC) es "el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial".

Troncoso refiere que "los datos de salud y la HC tienen una enorme importancia porque son instrumentos necesarios para garantizar la asistencia sanitaria de las personas" (11).

HISTORIA CLÍNICA ELECTRÓNICA

La historia clínica electrónica (HCE) es el registro electrónico de la HC, que puede ser consultado desde cualquier punto de asistencia del sistema sanitario. Es un instrumento que se considera imprescindible para la coordinación entre todos los niveles de la asistencia y asegura la continuidad en la atención por parte de los profesionales sanitarios (12). En España, la comunidad autónoma gallega fue la pionera en publicar el primer decreto regulador de la HCE, el Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica (13). Las ventajas de la HCE, según Pombo(14), recaen en una mayor centralización, seguridad, accesibilidad desde diferentes lugares, coherencia, disponibilidad, posibilidad de ser consultada por varias personas a la vez, control de acceso, reducción de costes administrativos, productividad e incluso explotación de datos.

TRATAMIENTO DE DATOS

Según el artículo 3 de la LOPD se entiende por tratamiento de datos a aquellas *"operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias"*. Para Hidalgo, en esencia, prácticamente toda interacción con un dato de carácter personal se considera tratamiento (15).

RESPONSABLE DEL FICHERO O DEL TRATAMIENTO

En el nuevo RGPD queda definido el responsable del tratamiento como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento".

Encargado del tratamiento

En el RGPD se define el encargado del tratamiento como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento"*.

MATERIAL Y MÉTODOS

Para contextualizar este trabajo y conseguir el objetivo propuesto, se llevó a cabo por un lado una búsqueda bibliográfica realizada a través de las bases de datos Enfispo, Índice Médico Español (IME), Bireme y Cuiden. Esta búsqueda en bases para la contextualización del trabajo se amplió a los últimos 10 años para incidir en su perspectiva histórica. Por otro lado, se efectuó un análisis de la página web de la Agencia Española de Protección de Datos (AEPD), que es la autoridad estatal de control independiente creada en 1992 y encargada de velar por el cumplimiento de la normativa sobre protección de datos. En la búsqueda a través de las bases de datos se utilizaron y se asociaron de forma combinada para aumentar los resultados de búsqueda los siguientes términos: "protección", "datos", "hospital" e "historia clínica". El análisis de la AEPD se realizó mediante el escrutinio de su página web en la que se examinaron documentos varios como informes, resoluciones y memorias, en búsqueda de información relacionada con el objetivo de esta investigación.

RESULTADOS

De la investigación en los archivos de la AEPD destacaron tres documentos que se analizarán a continuación: la Memoria de actividad de la AEPD de 1996, el Informe de cumplimiento de la LOPD en Hospitales de 2010 y el Plan de inspección sectorial de oficio de Hospitales Públicos, fechado en 2017.

MEMORIA DE 1996

En la memoria de actividad de la AEPD relativa al año 1996 (), en su apartado de Sanidad, se incluyeron las conclusiones del Plan Sectorial de Oficio diseñado el año anterior el cual se realizó con el objetivo de analizar el nivel de aplicación de la normativa de protección de datos en los hospitales públicos. De él se desprendía que las denuncias en años anteriores relativas al ámbito hospitalario habían sido en general escasas, estando relacionadas con posibles cesiones de datos o con el tratamiento de los mismos sin autorización para finalidades diferentes a las que motivaron su recogida. En este informe de 1996 se cuantificaron un total de once denuncias relacionadas con temas sanitarios, de las cuales solo cinco de ellas concernían a los hospitales públicos. Tres de estas cinco denuncias a hospitales se abrieron de oficio, tras la pertinente inspección, siendo otra denuncia relacionada con la cesión de los datos sin consentimiento del afectado y otra denuncia referente al derecho de acceso del mismo. Las restantes seis denuncias se recogen en la siguiente Tabla 1, donde se resumen los expedientes, organizados por tipo de denuncia y tipo de centro sanitario público:

Tabla 1. Tipos de denuncias en 1996 organizadas por tipos de centro. Fuente: AEPD.

TIPO DE DENUNCIA	TIPO DE CENTRO					TOTALES
	Hospitales	Consultas medicas	Organismos CC.AA.	Ayuntamientos	Otros	
Oficio	3		1			4
Cesión	1	1	1	1	1	5
Tratamiento		1				1
Acceso	1					1
TOTALES	5	2	2	1	1	11

En este informe de 1996, se destacaron los siguientes aspectos relacionados con la protección de datos:

- Los órganos directivos de los centros no tenían ni el cono-

cimiento ni la implicación necesaria en lo que a protección de datos se refería, ni una mentalización sobre los problemas de seguridad.

- Faltaban definiciones de nivel de confidencialidad de los datos que se utilizaban desde los distintos puntos de tratamiento de los centros.

- En materia de cesión de datos, faltaba una definición sobre los requisitos legales necesarios para su cesión a otros centros.

- No existían procedimientos sobre los tipos de datos que podían transferirse internacionalmente así como los posibles destinatarios.

- Faltaba un control de salida de datos de los centros.

- No estaban correctamente declarados los ficheros existentes.

- No existía un Plan de Seguridad ni conciencia respecto de los riesgos asociados a una seguridad deficiente.

- Por último, no se informaba a los usuarios:

a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

e) De la identidad y dirección del responsable del fichero.

INFORME DE CUMPLIMIENTO DE LA LOPD EN HOSPITALES, 2010.

La siguiente evaluación disponible sobre cumplimiento de la LOPD en hospitales, fue el Informe de cumplimiento de la LOPD en Hospitales de 2010(). La evaluación se realizó mediante el envío de un cuestionario a 292 hospitales públicos, además de a otros 313 de titularidad privada, incluidos en el Catálogo Nacional de Hospitales. Ya en este informe se constató el incremento en el número de reclamaciones relacionadas con los derechos de acceso, rectificación, cancelación y oposición sobre las historias clínicas, planteadas por ciuda-

danos que no habían sido atendidos adecuadamente en los centros hospitalarios. Se mencionaba además el incremento de procedimientos tramitados por la AEPD relacionados con la vulneración de los deberes de seguridad y secreto por parte de centros sanitarios. Concretamente, en 2009 se registraron un total de 123 denuncias y actuaciones previas de investigación en el sector de la sanidad. También destacó que, comparativamente, el nivel de cumplimiento de la LOPD en los centros públicos fue menor que en los centros privados (las mayores diferencias de cumplimiento comparados con los privados se presentaron en las cláusulas informativas de los formularios de recogida de datos y en las auditorías bienales de seguridad). A continuación se muestran algunos resultados en los hospitales públicos sobre los temas evaluados:

1. Sobre la obligatoria inscripción de ficheros en el Registro General de Protección de Datos, destacaron dos datos. Por un lado, el 89 % de los hospitales confirmaron que habían realizado tal inscripción, aunque menos, el 80 % de éstos, mantenían actualizada la inscripción.

2. Del deber de información al interesado y atención al ejercicio de derechos de acceso, rectificación, cancelación y oposición (ARCO), varios resultados llamaban la atención. Por ejemplo, se constató que solo en el 55% de los hospitales se incluía una clausula informativa sobre estos derechos en los formularios de recogida de datos de los pacientes y usuarios. Este porcentaje aumentaba ligeramente al 64% cuando se trataba de comprobar la existencia de carteles informativos sobre el derecho de protección de datos personales a disposición de los pacientes y usuarios del centro. Donde sí mejoraba el porcentaje era en que el 84% de hospitales disponían de procedimientos definidos para atender a las personas que solicitaban el ejercicio del derecho de acceso, rectificación, cancelación y oposición en la entrega de sus datos

3. En cuanto a la contratación de servicios con tratamiento de datos personales, también destacaron varios resultados. Así, se confirmó que el 83% de los hospitales tenía contratada o externalizada la prestación de ciertos servicios con tratamiento de datos personales para, por ejemplo, la custodia de las HCs, la destrucción de documentos, el mantenimiento informático o las pruebas analíticas en laboratorios externos al centro. Sin em-

bargo, solo un 37% de estos centros aplicaban procedimientos de disociación de datos que impidieran la identificación de las personas por parte de las empresas externas al hospital. Por otro lado, el 74% de los hospitales afirmaron que mantenían informado al personal de limpieza sobre la necesidad de garantizar la confidencialidad de los datos, por ejemplo, en la recogida de la basura.

4. En cuanto a las medidas de seguridad, más del 92% de los centros afirmaron disponer de medidas técnicas para impedir el acceso o difusión de los datos por parte de terceros no autorizados; tener definidas las funciones y obligaciones del personal y cerciorarse que el personal conociese sus obligaciones sobre la protección de datos. Este dato contrastaba con el que se obtenía cuando a esos mismos hospitales se les preguntaba si formaban a su personal sobre la protección de datos, un 74% solamente. En cuanto a otras medidas de seguridad, en el 96% de los hospitales los usuarios se identificaban mediante clave y contraseña para el acceso a los datos y en el 95% de ellos el personal solo podía acceder a datos o recursos autorizados.

5. Sobre la existencia de auditorías de medidas de seguridad, este informe arrojó que solo en un 25% de los centros se auditaba si el personal autorizado utilizaba los datos para la finalidad que justificó el acceso, o que un 45% de los centros había realizado la preceptiva auditoria bienal de seguridad del Fichero de Historias Clínicas. Como dato positivo, el 95% de ellos afirmaba que los locales en los que se encontraban los dispositivos de almacenamiento se cerraban cuando no había personal de la organización para su custodia.

Por los resultados obtenidos, las recomendaciones que la AEPD realizó a los centros, independientemente del obligado cumplimiento que debían hacer de la ley, fueron las siguientes:

- Actualizar la inscripción de los ficheros de datos de carácter personal.
- Publicar y actualizar en el diario oficial correspondiente la pertinente disposición general de adecuación a la LOPD y al RLOPD para los ficheros de titularidad pública.
- Incluir en los formularios de recogida de datos de los pacientes y usuarios cláusulas in-

formativas respecto al tratamiento de datos personales, adaptándolas en cada formulario en función del fichero en el que se van a incluir los datos y/o finalidad para la que van a ser utilizados (asistencia sanitaria, epidemiología, investigación, docencia, evaluación de la calidad asistencial, etc.).

- Colocar en lugares visibles carteles informativos sobre el derecho a la protección de datos personales de los usuarios del centro.

- Informar al personal de limpieza sobre la necesidad de garantizar la confidencialidad de los datos (por ejemplo, en la recogida de la basura).

- Disociar los datos cuando se realice un tratamiento externalizado de datos personales.

- Registrar todos los accesos a la HC, almacenando la información de cada uno de ellos durante un periodo no inferior a dos años.

- Realizar auditorías que verifiquen si el personal autorizado utiliza los datos para la finalidad que justificó el acceso.

- Archivar las HCs en lugares protegidos bajo llave o dispositivo similar y en archivadores que dispongan de mecanismos que dificulten su apertura.

- Custodiar de forma segura la HC, para evitar accesos no autorizados, cuando ésta abandone los archivos para ser consultada.

- Adoptar medidas que eviten la sustracción, pérdida o acceso indebido a los datos durante su transporte.

- Auditar cada dos años la seguridad del archivo de las HCs y de otros archivos con datos de salud, ejecutando medidas correctoras ante las deficiencias encontradas.

PLAN DE INSPECCIÓN SECTORIAL DE OFICIO DE HOSPITALES PÚBLICOS, 2017

El tercer documento hallado y analizado fue el Plan de Inspección Sectorial de Oficio de Hospitales Públicos(), de 2017, que surgió por la necesidad de evaluar el grado de implementación de las recomendaciones que la Agencia realizó en evaluaciones previas. Esta evaluación específica de los hospitales públicos se enmarcó dentro del Plan estratégico 2015-2019 de la AEPD (), en el Eje estratégico 1 llamado “Prevención para una protección más eficaz”, el cual incluye un programa dedicado a la sanidad. Con los resultados derivados de

este informe, la AEPD ofrecía un punto de referencia para que el sector sanitario abordase la adaptación de sus sistemas y procedimientos a los nuevos requerimientos que actualmente impone a nivel europeo el RGPD.

El contenido del informe provino de inspecciones presenciales a los hospitales que fueron anteriormente auditados y a aquellos de nueva creación. La exposición de los resultados de este informe no se hizo de forma cuantitativa indicando los porcentajes de cumplimiento de los diferentes indicadores estudiados, sino con expresiones del tipo *"en la mayoría de los centros…"*, "*con carácter general…", "varios de los hospitales visitados…"*, etc. En varios de los hospitales auditados se realizaron también comprobaciones sobre los procedimientos de investigación médica y el correspondiente tratamiento de los datos personales que se efectuaban sobre este tema. A continuación se sintetizan algunos aspectos destacados a nivel asistencial y de investigación, especialmente aquellos en los que enfermería tiene una implicación directa y que resultan necesarios conocer.

RECOMENDACIONES A NIVEL ASISTENCIAL

- Conservar los datos un mínimo de 5 años desde el alta del proceso asistencial o más tiempo si así lo marca la ley autonómica correspondiente. Esto es así porque en algunos centros no se procedía al borrado, cancelación o bloqueo de datos, almacenándose los datos indefinidamente, entendiendo que la historia no debe ser eliminada por motivos asistenciales, ni tampoco se destruían las historias en papel.

- Mantener siempre los datos relacionados con el nacimiento y que sirvan para demostrar el vínculo de filiación entre madre e hijo. Nunca deben destruirse.

- Incluir los derechos ARCO en los formularios de recogida de información y también en los consentimientos informados.

- No colocar la lista de pacientes de la consulta en un lugar a la vista de todo el público, utilizando tickets codificados en las consultas para atender al paciente, debido a que en las consultas de algunos hospitales se seguía llamando por megafonía al paciente por su nombre y apellidos.

- Obtener el consentimiento del paciente si desea o no que sea facilitada información sobre su ubicación en el hospital a personas o familiares, ya que existía confusión y preocupación en los hospitales a la hora de determinar en qué situaciones se puede dar información sobre la ubicación de un paciente a

una persona que acuda al hospital a preguntar por el paciente. En todo caso el centro no debe proporcionar datos de salud o de la atención prestada.

- Realizar las comunicaciones entre hospitales y centros de salud con seguridad alta. No está permitida la remisión de datos de salud vía fax sin cifrado.

- Las HCs deben quedar almacenadas en salas cerradas, bajo llave (sin dejarla puesta) identificando al responsable de su custodia, informando sobre las responsabilidades en las que se puede incurrir en caso de no observar su custodia. La HC en papel de algunos hospitales se almacenaba en lugares abiertos, en archivadores sin cerraduras.

- No almacenar copias de documentos en ordenadores personales aunque estén dentro del propio servicio, porque están fuera de la política de copias de seguridad del hospital

3.3.2. Recomendaciones sobre investigación.

- Se debe solicitar siempre el consentimiento informado para la participación en el estudio, o si esto precisara de un esfuerzo desproporcionado, establecer un mecanismo que preserve la identidad del participante. En ocasiones, el personal sanitario podía acceder a las HCs para la revisión retrospectiva de los casos, sin el marco de una investigación auditada por el Comité Ético de Investigación Médica o una comisión de investigación.

- En el acceso a las salas de lectura de documentación clínica, se debe registrar quién accede y las HCs deben estar en lugar cerrado bajo llave.

- El hospital debe custodiar bajo sus propias medidas de seguridad, incluso si son de participantes que no tengan HC previa en el hospital, el documento donde se recoge los datos identificativos de los participantes junto con sus códigos de participación, ya que en algunos hospitales estaba en posesión del investigador principal.

- Los consentimientos informados para la investigación deben tener información sobre la protección de datos: qué ocurre con la información al acabar el estudio, la codificación de los datos, las medidas de seguridad aplicables, los derechos ARCO, el abandono anticipado del estudio, etc.

CONCLUSIONES

Con el análisis de estos documentos se ha constatado el profundo cambio que ha habido en los hospitales públicos españoles, desde aquel primer informe de 1996 hasta este último del año 2017. Los sucesivos informes han puesto de manifiesto que conforme han

pasado los años, bien sea por el aumento de la legislación, bien sea por la adquisición de la cultura de protección de datos por parte de los propios profesionales, el respeto a este derecho fundamental recogido acertadamente en la Constitución española ha ido en aumento. En este sentido, la formación continuada del personal sanitario relativa a este tema ha jugado un papel importante. Esta formación consideramos que debe dirigirse a todos los trabajadores del centro ya que la importancia del tratamiento correcto de los datos personales de los pacientes es competencia de todos los trabajadores del hospital. Los profesionales debemos conocer la normativa, lo que nos dará mayor seguridad en el trabajo, hacia nosotros y hacia el paciente, aumentando la calidad de nuestra asistencia. En este sentido, recomendamos la lectura de diversas resoluciones de la AEPD en las que los profesionales de enfermería se han visto involucrados, como por ejemplo, situaciones relacionadas con la custodia del fichero de datos personales (20), el acceso a datos sin autorización del titular (21,22), o la exposición pública del listado de pacientes de consulta (23).

Por otro lado y como se aludió anteriormente, los hospitales públicos deben mejorar su cumplimiento de la protección de datos en los aspectos citados con respecto a los hospitales privados. Este mayor cumplimiento en el sector privado puede deberse a que en el sector público puede existir una idea generalizada de que la responsabilidad queda diluida en el propio sistema, que somos todos, no así en el privado, donde la falta de responsabilidad puede afectar directamente a la viabilidad económica de la actividad empresarial. Otros aspectos a mejorar en el sector público deben ser el aumento de carteles informativos sobre protección datos, las revisiones del documento de seguridad, el registro de los accesos a los datos e impedir la falta de seguridad en la custodia de las historias clínicas en papel, especialmente durante su transporte.

Es necesario recalcar que en paralelo a la generalización de la HCE, los datos de salud actualmente se enfrentan a una revolución digital que se está viviendo en el conjunto de la sociedad, en la que la información sobre las personas ha crecido enormemente tanto en cantidad como en conectividad. Todo ello nos plantea nuevos retos para la protección de datos de salud, más aún cuando el acceso y uso compartido entre diferentes instituciones sanitarias debe considerarse imprescindible para prestar una mejor asistencia a las personas. A modo de mejora digital, es imprescindible aumentar el uso de la HCE en aquellos lugares

donde todavía no se encuentre completamente instaurada, ya que su uso es inevitable en la actualidad, dotando de los recursos necesarios tanto humanos, materiales y financieros para su implantación.

Quedan otros retos pendientes, como por ejemplo la adaptación del nuevo RGPD al sistema sanitario, el cual vendrá a darnos mayor protección a los usuarios. Es necesario recalcar además que debido a esta circunstancia actualmente existe un nuevo Proyecto De Ley Orgánica de Protección de Datos de Carácter Personal (24), que vendrá a perfeccionar la actual LOPD y a reforzar la protección de los derechos de los ciudadanos. En lo que afecta al ámbito hospitalario, los responsables y encargados del tratamiento deberán tener designado un delegado de protección de datos y sería interesante analizar en el futuro cómo evoluciona su cumplimiento.

BIBLIOGRAFÍA

1. Constitución Española. Boletín Oficial del Estado no 311 de 29 de diciembre de 1978.
2. Álvarez J. Guía práctica sobre protección de datos. Madrid: Lex Nova; 2011. p. 54.
3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado no 298 de 14 diciembre de 1999.
4. Ministerio de Sanidad, Servicios Sociales e Igualdad [Internet] Madrid: MSSSI; [consultado 24 sep 2019]. Disponible en: https://www.mscbs.gob.es/ciudadanos/prestaciones/centrosServiciosSNS/hospitales/docs/2018_CNH.pdf
5. Canales A. La protección de datos y su repercusión en el mundo sanitario. En: Cuadernos del Observatorio de Salud en Europa sobre políticas de salud en la UE. Sevilla: Observatorio de Salud en Europa de la Escuela Andaluza de Salud Pública, no2; 2008. p. 2.
6. Colegio de Enfermería de Sevilla [Internet] Sevilla; [consultado 17 ene 2019]. Disponible en: http://colegioenfermeriasevilla.es/wp-content/uploads/CODIGO_DEONTOLOGICO.pdf
7. 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 de 19 de enero de 2008.
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 (RGPD). Diario Oficial de la Unión Europea nº 119 de 4 de mayo de 2016.
9. 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. Boletín Oficial del Estado no 274 de 15 de noviembre de 2002.
10. Gómez Y. Datos de salud como datos especialmente protegidos. En: Troncoso A, director. Comentarios a la Ley Orgánica de Protección de datos de carácter personal. Navarra: Aranzadi; 2010. p. 649. 11
11. Troncoso A. La protección de datos personales. En busca del equilibrio. Valencia: Tirant lo Blanch; 2010. p. 1099.
12. Galimany J. Enfermería y nuevas tecnologías. Historia clínica electrónica. Rev ROL Enferm. 2012; 35(9): 602-5.
13. Sánchez-Caro J. La historia clínica electrónica gallega: un paso importante en la gestión del conocimiento. Derecho y Salud. 2009; 18(1): 57-85.
14. Pombo N. Algunas claves de gestión clínica. La Fundación Hospital de Alcorcón. En: Jiménez J, director. Manual para Jefes de Gestión de Servicios Clínicos. 2a ed. Madrid: Díaz de Santos; 2000. p. 261.
15. Hidalgo A. Protección de datos de carácter personal relativos a la salud del paciente: fundamentos, protección a la intimidad y comentarios al nuevo Reglamento UE 2016/679. RDUNED. 2016; 19: 715-44.
16. Agencia Española de Protección de datos [Internet] Madrid: AEPD; [consultado 1 mar 2018]. Disponible en: https://www.aepd.es/media/memorias/memoria-AEPD-1996.pdf
17. Agencia Española de Protección de datos. Informe de cumplimiento de la LOPD en Hospitales. Madrid: Agencia Española de Protección de datos; 2010.
18. Agencia Española de Protección de datos [Internet] Madrid: AEPD; [consultado 17 abr 2018]. Disponible en: https://www.aepd.es/media/planes/plan-de-inspeccion-hospitales-publicos.pdf
19. Agencia Española de Protección de datos [Internet] Madrid: AEPD; [consultado 20 mar 2018]. Disponible en: https://www.aepd.es/agencia/transparencia/common/plan-estrategico/plan-estrategico-AEPD.pdf
20. Agencia Española de Protección de datos [Internet] Madrid: AEPD; [consultado 17 ene 2019]. Disponible en: https://www.aepd.es/resoluciones/AAPP-00012-2012_ORI.pdf
21. Agencia Española de Protección de datos [Internet] Madrid: AEPD; [consultado 18 ene 2019]. Disponible en: https://www.aepd.es/resoluciones/AAPP-00037-2013_ORI.pdf
22. Agencia Española de Protección de datos [Internet] Madrid: AEPD; [consultado 17 ene 2019]. Disponible en: https://www.aepd.es/resoluciones/AAPP-00041-2017_ORI.pdf
23. Agencia Española de Protección de datos [Internet] Madrid: AEPD; [consultado 19 ene 2019]. Disponible en: https://www.aepd.es/resoluciones/AAPP-00020-2013_ORI.pdf
24. Proyecto De Ley Orgánica de Protección de Datos de Carácter Personal. Boletín Oficial de las Cortes Generales no 13-1 de 24 de noviembre de 2017.