Informe de cumplimiento de la LOPD en Hospitales

Agencia Española de Protección de Datos

Octubre de 2010

1. INTRODUCCIÓN

La Agencia Española de Protección de Datos (AEPD) ha observado últimamente un incremento en las reclamaciones relativas al ejercicio de los derechos de acceso, rectificación, cancelación y oposición en relación con las Historias Clínicas, planteadas por ciudadanos que no han sido atendidos adecuadamente en centros hospitalarios, así como del número de procedimientos tramitados por la Agencia vinculados a la vulneración de los deberes de seguridad y secreto por parte de centros sanitarios. En particular, en 2009 se registraron un total de 123 denuncias y actuaciones previas de investigación en el sector de la sanidad.

Dada la importancia de estos tratamientos de datos y la trascendencia del derecho fundamental a la protección de datos en este sector, en el mes de marzo de 2010 la Agencia tomó la iniciativa de elaborar el ***Informe de cumplimiento de la LOPD en Hospitales*** y remitirlo a cada uno de los centros públicos y privados que componen el Catálogo Nacional de Hospitales, al objeto de conocer el nivel de cumplimiento de la LOPD y de su normativa de desarrollo en centros hospitalarios, para adoptar las medidas que resultasen pertinentes.

2. MARCO LEGAL APLICABLE

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y su Reglamento de desarrollo, aprobado mediante Real Decreto 1720/2007 de 21 de diciembre (RLOPD), establecen el marco general que regula el derecho fundamental de protección de datos.

La actuación de la AEPD en relación con el citado ***Informe de cumplimiento de la LOPD en Hospitales*** está basado en las funciones que le confiere el artículo 37.1 de la LOPD. En particular, las de "*velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación*" (art. 37.1 a), "*requerir a los responsables y encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación de los tratamientos de datos a las disposiciones de la Ley*" (art. 37.1 f), así como "*recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones*" (37.1 i).

Debe recordarse que los tratamientos de datos de carácter personal que se realizan en el ámbito hospitalario y, en particular, los relacionados con la gestión de las historias clínicas o la investigación clínica, incluyen datos de salud, considerados datos sensibles o especialmente protegidos y, como tales, tienen un régimen de garantías más reforzado. En este sentido, conforme a lo dispuesto en los artículos 7.3 y 44.4 de la LOPD y el artículo 81 del RLOPD, este mayor nivel de garantías se concreta en la exigencia de un consentimiento reforzado, la

cualificación de las infracciones como muy graves y la aplicación de las medidas de seguridad de nivel alto especificadas en el propio reglamento.

Por otra parte, los principios de respeto a la intimidad y a la confidencialidad de la información clínica de los pacientes están presentes asimismo en la legislación sanitaria. La regulación del derecho a la protección de la salud, recogido por el artículo 43 de la Constitución de 1978, desde el punto de vista de las cuestiones más estrechamente vinculadas a la condición de sujetos de derechos de las personas usuarias de los servicios sanitarios, es decir, la plasmación de los derechos relativos a la información clínica y la autonomía individual de los pacientes en lo relativo a su salud, fue objeto de una regulación básica en el ámbito del Estado, a través de la Ley 14/1986, de 25 de abril, General de Sanidad. Esta Ley, a pesar de que fija básicamente su atención en el establecimiento y ordenación del sistema sanitario desde un punto de vista organizativo, dedica a esta cuestión diversas previsiones, entre las que destaca la voluntad de humanización de los servicios sanitarios. Así, mantiene el máximo respeto a la dignidad de la persona y a la libertad individual, de un lado, y, del otro, declara que la organización sanitaria debe permitir garantizar la salud como derecho inalienable de la población mediante la estructura del Sistema Nacional de Salud, que debe asegurarse en condiciones de escrupuloso respeto a la intimidad personal y a la libertad individual del usuario, garantizando la confidencialidad de la información relacionada con los servicios sanitarios que se prestan. Esta norma se complementa con las previsiones de la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.

Por su parte, 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, completa las previsiones que la Ley General de Sanidad enunció como principios generales. Así, recoge entre sus principios básicos que la persona que elabore o tenga acceso a la información y documentación clínica está obligada a guardar la reserva debida (art. 2.7), al mismo tiempo que establece el derecho que toda persona tiene a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley (art. 7.1).

En su artículo 14, la Ley 41/2002 regula el archivo de las historias clínicas de los pacientes, estableciendo que, cualquiera que sea el soporte en el que consten, debe quedar garantizada su seguridad, su correcta conservación y la recuperación de la información.

En relación con los usos de la historia clínica, el artículo 16 de la Ley 41/2002 establece que su finalidad principal es garantizar la adecuada asistencia sanitaria al paciente, compatible con otros usos de interés general, así como que el personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones, añadiendo que el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto. Al mismo tiempo, regula en su artículo 18 el derecho de acceso del paciente a su historia clínica y a obtener copia de los datos que figuren en ella, asignando a los centros sanitarios la responsabilidad de regular el procedimiento que garantice la observancia de estos derechos.

Por último, es de destacar que en lo concerniente a la conservación de la documentación clínica, la Ley 41/2002 hace en su artículo 17 una referencia explícita a la LOPD y a su normativa de desarrollo, al establecer que "*son de aplicación las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contiene datos de carácter personal y, en general, por La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal*".

3. ALCANCE Y METODOLOGÍA

La evaluación del nivel de cumplimiento de la normativa de protección de datos personales se ha realizado mediante el envío a los centros sanitarios incluidos en el Catálogo Nacional de Hospitales que se encuentran bajo la competencia de esta Agencia, consistente en un cuestionario del que se ha requerido su cumplimentación.

A tal efecto, el 26 de marzo se envió un primer requerimiento solicitando su contestación antes del 31 de mayo. Con fecha 18 de junio se les reiteró a aquellos hospitales de los que no se había recibido contestación, ampliando el plazo para su contestación hasta el 31 de julio de 2010. En esta segunda comunicación, se advertía expresamente que en caso contrario se procedería a dar traslado del hecho al órgano encargado de la función inspectora y sancionadora por posible infracción conforme al artículo 44.2.b) de la LOPD.

La relación de centros hospitalarios objeto del requerimiento se ha obtenido a partir del Catálogo de Hospitales 2009, publicado en la página web del Ministerio de Sanidad y Política Social a fecha 1 de marzo de 2010. El Catálogo Nacional de Hospitales es fruto de la colaboración entre el Ministerio de Sanidad y Política Social y las Consejerías de Sanidad de las Comunidades Autónomas, el Ministerio de Defensa, los órganos competentes de las Ciudades Autónomas de Ceuta y Melilla y los propios Hospitales. Su marco legal viene definido por la Ley 14/1986, de 25 de abril, General de Sanidad, que atribuye al Estado entre sus actuaciones *"El Catálogo y Registro General de centros, servicios y establecimientos sanitarios que recogerán las decisiones, comunicaciones y autorizaciones de las Comunidades Autónomas, de acuerdo con sus competencias"* (Art. 40.9). Asimismo, la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud establece en su artículo 53.2 que "*El sistema de información sanitaria contendrá información sobre las prestaciones y la cartera de servicios en atención sanitaria pública y privada, e incorporará, como datos básicos, los relativos a población protegida, recursos humanos y materiales…*".

El objetivo de este Catálogo es ofrecer información básica de los hospitales existentes en el conjunto del territorio nacional a las personas e instituciones interesadas en el conocimiento del sector, tales como Administración Sanitaria, estudiosos, usuarios, proveedores de servicios, etc. El Catálogo recoge información de los centros sanitarios destinados a la asistencia especializada y continuada de pacientes en régimen de internado, cuya finalidad principal es el diagnóstico y/o tratamiento de los enfermos ingresados en el mismo, así como la atención a pacientes de forma ambulatoria.

El requerimiento fue enviado a los 654 centros que se encuentran en el ámbito de competencia de la Agencia Española de Protección de Datos. Por lo tanto, no han sido objeto de esta actuación los centros de las Comunidades Autónomas de Madrid, Cataluña y del País Vasco, que se encuentran bajo control de las Agencias de Protección de Datos de Madrid, Cataluña y País Vasco, respectivamente.

El colectivo de centros objeto del estudio se ha circunscrito a 605, al haber sido eliminados aquellos centros para los que se producían algunas duplicidades en el Catálogo, o bien habían cesado su actividad.

Una vez finalizados los plazos de requerimiento señalados se ha recibido la contestación de 562 centros (92,9% del total), distribuidos por Comunidad Autónoma en la forma que se muestra en la Tabla 1.

Comunidad Autónoma	Centros requeridos	Centros contestados	% Centros contestados
CIUDAD AUTÓNOMA DE CEUTA	2	2	100,00
CIUDAD AUTÓNOMA DE MELILLA	1	1	100,00
C.A. DE ANDALUCÍA	124	119	95,97
C.A DE ARAGÓN	29	27	93,10
C.A. DE CANARIAS	42	35	83,33
C.A. DE CANTABRIA	9	8	88,89
C.A. DE CASTILLA Y LEÓN	50	49	98,00
C.A. DE CASTILLA-LA MANCHA	33	28	84,85
C.A. DE EXTREMADURA	26	24	92,31
C.A. DE GALICIA	63	53	84,13
C.A. DE LA REGIÓN DE MURCIA	26	26	100,00
C.A. DE LA RIOJA	7	7	100,00
C.A. DE LES ILLES BALEARS	23	20	86,96
C.A. DEL PAÍS VASCO	26	24	92,31
C.A. DEL PRINCIPADO DE ASTURIAS	23	23	100,00
COMUNIDAD DE MADRID	48	47	97,92
COMUNIDAD FORAL DE NAVARRA	13	13	100,00
COMUNIDAD VALENCIANA	60	56	93,33
TOTAL GENERAL	**605**	**562**	**92,89**

Tabla 1 Número de centros hospitalarios requeridos por Comunidad Autónoma

En las Tablas 2 y 3 se puede observar la distribución por Comunidad Autónoma de las contestaciones en función de la titularidad pública o privada de los centros, respectivamente.

CENTROS DE TITULARIDAD PÚBLICA

Comunidad Autónoma	Centros requeridos	Centros contestados	% Centros contestados
CIUDAD AUTÓNOMA DE CEUTA	1	1	100,00
CIUDAD AUTÓNOMA DE MELILLA	1	1	100,00
C.A. DE ANDALUCÍA	67	65	97,01
C.A. DE ARAGÓN	19	18	94,74
C.A. DE CANARIAS	17	13	76,47
C.A. DE CANTABRIA	5	4	80,00
C.A. DE CASTILLA Y LEÓN	26	26	100,00
C.A. DE CASTILLA-LA MANCHA	22	19	86,36
C.A. DE EXTREMADURA	18	17	94,44
C.A. DE GALICIA	39	31	79,49
C.A. DE LA REGIÓN DE MURCIA	10	10	100,00
C.A. DE LA RIOJA	5	5	100,00
C.A. DE LES ILLES BALEARS	11	11	100,00
C.A. DEL PAÍS VASCO	0	0	0,00
C.A. DEL PRINCIPADO DE ASTURIAS	12	12	100,00
COMUNIDAD DE MADRID	0	0	0,00
COMUNIDAD FORAL DE NAVARRA	6	6	100,00
COMUNIDAD VALENCIANA	33	29	87,88
TOTAL GENERAL	**292**	**268**	**91,78**

Tabla 2: Número de centros públicos requeridos por Comunidad Autónoma

CENTROS DE TITULARIDAD PRIVADA

Comunidad Autónoma	Centros requeridos	Centros contestados	% Centros contestados
CIUDAD AUTÓNOMA DE CEUTA	1	1	100,00
CIUDAD AUTÓNOMA DE MELILLA	0	0	0,00
C.A. DE ANDALUCÍA	57	54	94,74
C.A. DE ARAGÓN	10	9	90,00
C.A. DE CANARIAS	25	22	88,00
C.A. DE CANTABRIA	4	4	100,00
C.A. DE CASTILLA Y LEÓN	24	23	95,83
C.A. DE CASTILLA-LA MANCHA	11	9	81,82
C.A. DE EXTREMADURA	8	7	87,50
C.A. DE GALICIA	24	22	91,67
C.A. DE LA REGIÓN DE MURCIA	16	16	100,00
C.A. DE LA RIOJA	2	2	100,00
C.A. DE LES ILLES BALEARS	12	9	75,00
C.A. DEL PAÍS VASCO	26	24	92,31
C.A. DEL PRINCIPADO DE ASTURIAS	11	11	100,00
COMUNIDAD DE MADRID	48	47	97,92
COMUNIDAD FORAL DE NAVARRA	7	7	100,00
COMUNIDAD VALENCIANA	27	27	100,00
TOTAL GENERAL	**313**	**294**	**93,93**

Tabla 3: Número de centros privados requeridos por Comunidad Autónoma

Mediante la cumplimentación del ***Informe de cumplimiento de la LOPD en Hospitales*** los centros sanitarios requeridos han notificado su situación respecto a los siguientes aspectos:

- Inscripción de ficheros en el Registro General de Protección de Datos

- Deber de información al interesado y atención al ejercicio de derechos de acceso, rectificación, cancelación y oposición (ARCO)
- Contratación de servicios de tratamiento de datos personales[1]
- Medidas de seguridad y, específicamente sobre el documento de seguridad; funciones y obligaciones del personal; control y registro de acceso; comunicación de datos; gestión de incidencias; gestión de soportes y documentos; copias de respaldo y recuperación; y documentación en papel.
- Auditoría de medidas de seguridad

4. RESULTADOS GLOBALES

El análisis de resultados que se detalla en los siguientes apartados del documento se refiere a la muestra de centros que han remitido una contestación válida.

4.1 INSCRIPCIÓN DE FICHEROS EN EL RGPD

El nivel de cumplimiento de la LOPD declarado por los centros hospitalarios en materia de inscripción de ficheros es el siguiente:

- El 94,4% ha inscrito los ficheros de datos personales en el RGPD, y un 88,3% mantiene estas inscripciones actualizadas.
- El 83,8% de los centros de titularidad pública ha publicado la disposición general de creación de ficheros en el diario oficial correspondiente.
- El 90,7% de los centros tiene inscrito el fichero de Historias Clínicas de Pacientes.
- Un 39,75% de los centros ha inscrito ficheros con la finalidad de Investigación Clínica, un 86,9% con la de Gestión Sanitaria, y un 89,9% ha inscrito ficheros relacionados con la gestión interna del centro (recursos humanos, proveedores, etc.)
- Un 71,9% ha inscrito ficheros con finalidades distintas a las indicadas anteriormente.
- El 55% de los centros han implantado la Historia Clínica Electrónica.

Los datos referidos al porcentaje de centros que tienen inscritos sus ficheros de datos de carácter personal han sido contrastados por esta Agencia, verificándose su adecuación con la información presente en el Registro General de Protección de Datos.

[1] En relación con el art. 12 de la LOPD

4.2 DEBER DE INFORMACIÓN AL INTERESADO Y ATENCIÓN AL EJERCICIO DE DERECHOS ARCO

- En los formularios de recogida de datos de los pacientes, un 24,3% de los centros no ha incluido una cláusula informativa conforme a lo establecido en el artículo 5 de la LOPD. Asimismo, en un 36,6% de los centros esta cláusula no está adaptada 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.

- Un 72,5% de los centros cuentan con carteles informativos sobre el derecho de protección de datos personales a disposición de los pacientes y usuarios del centro.

- El 90,7% de los centros disponen de procedimientos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición por parte de las personas que lo solicitan. En el 84,9% de los casos, la atención de estos derechos se encuentra centralizada en una Unidad del Centro Hospitalario.

- En el 70,5% de los centros, cuando se ejerce el derecho de reserva de las anotaciones subjetivas que constan en la Historia Clínica, la decisión sobre los datos que se facilitan es tomada por el profesional sanitario.

4.3 *CONTRATACIÓN DE SERVICIOS DE TRATAMIENTO DE DATOS PERSONALES*

La contratación o externalización de servicios de tratamiento de datos está ampliamente extendida en los Centros Hospitalarios (por ejemplo, para la realización de análisis clínicos u otras pruebas médicas, o para el almacenamiento de las historias clínicas), habiendo optado un 86% de ellos por este modelo de gestión. El 98,5% de los centros que han contratado este tipo de servicios han incluido las garantías de protección de datos previstas en el artículo 12 de la LOPD en el contrato de prestación de servicios.

Es relevante que sólo un 39,1% de los centros que han contestado declaran que emplean procedimientos de disociación de los datos de carácter personal.

Por otra parte, en el 84,5% de los centros se informa al personal de limpieza sobre la necesidad de garantizar la confidencialidad de los datos (por ejemplo, en la recogida de la basura).

4.4 MEDIDAS DE SEGURIDAD

En relación con las medidas de seguridad de los datos de carácter personal, el nivel de cumplimiento de la normativa es el siguiente:

Documento de seguridad

- Un 90,8% de los centros disponen de documento de seguridad; aunque sólo el 82,7% lo revisa periódicamente y mantiene actualizado.

Medidas básicas

En términos generales, el nivel de cumplimiento de las medidas de seguridad de nivel básico podría considerarse óptimo:

- En el 95,5% de los centros se encuentran definidas las funciones y obligaciones del personal. En particular, en el 94,4% de los centros sanitarios el personal está informado de su obligación de custodiar la documentación cuando ésta no se encuentra archivada en los dispositivos de almacenamiento por estar en revisión o tramitación. Asimismo, en el 79,7% de los hospitales se realizan actividades de formación del personal sobre protección de datos.

- El 88% de los hospitales dispone de procedimientos de notificación y gestión de incidencias que afecten a los datos de carácter personal.

- En el 96,8% de los centros hospitalarios se encuentra limitado el acceso a los datos, de forma que los usuarios no puedan acceder a datos o recursos distintos de los autorizados. El porcentaje de aquellos que además mantienen actualizada la relación de usuarios que tienen acceso autorizado a los datos personales es ligeramente inferior, alcanzando el 93,2% de los casos. Por otra parte, en el 88,4% de los centros el personal de gestión y control sanitario tiene limitado el acceso a las Historias Clínicas de los pacientes.

- La mayoría de centros sanitarios (94,8%) han implantado medidas técnicas que impiden el acceso de terceros no autorizados o la difusión de datos de carácter personal de los ficheros del centro sanitario (limitación de la descarga de programas de intercambio de archivos, cortafuegos, etc.)

- Sin embargo, es menor, sólo en el 81,1% de centros las salidas de soportes y documentos que contienen datos de carácter personal se encuentran debidamente autorizadas, mientras que en el 78,6% se han adoptado medidas para evitar la sustracción, pérdida o acceso indebido a la documentación durante su transporte (ej. traslado de las historias clínicas).

- La identificación de los usuarios mediante una clave de acceso y una contraseña está implantada en el 96,9% de los hospitales.

- El 96,6% de los hospitales ha definido procedimientos de copias de respaldo y de recuperación de los datos.

- Únicamente el 45% de los centros auditan que el personal autorizado ha utilizado los datos para la finalidad que justificó el acceso.

Medidas de nivel alto

- En el 88,7% de los centros hospitalarios las medidas previstas en el documento de seguridad son las correspondientes al nivel alto, que son las aplicables para los datos relativos a la salud de las personas.

- Sin embargo, la implantación de algunas de las medidas de seguridad exigidas en el RLOPD para los datos de nivel alto es inferior al porcentaje que declara haberlas previsto en el documento de seguridad. Así, el porcentaje de hospitales que dispone de un registro de accesos a toda la información es del 74,6%, mientras que el nivel de hospitales en los que se guarda la información exigida por el RLOPD de cada acceso realizado a los datos (identificación del usuario, fecha y hora del acceso, fichero accedidos, tipo de acceso e indicación de acceso autorizado o denegado) es ligeramente inferior, alcanzando el 70,5%. Es reseñable igualmente el hecho de que un 31% de los centros no almacena el registro de acceso durante el periodo mínimo preceptivo de dos años.

Ficheros manuales

- Un 22,1% de los centros no cuentan con dispositivos de almacenamiento de historias clínicas dotados de mecanismos que obstaculicen su apertura (p.ej. archivadores con cerradura).

- En el 96,6% de los hospitales, los locales en los que se encuentran los dispositivos de almacenamiento se encuentran cerrados cuando no hay personal de la organización a su cargo.

- El 96% de los centros disponen de medios de destrucción y desecho de la información que garantizan la confidencialidad de la información e imposibilitan su acceso a terceros no autorizados.

4.5 AUDITORÍA DE MEDIDAS DE SEGURIDAD

La realización de la auditoría bienal de seguridad del fichero de Historias Clínicas es uno de los aspectos en los que se observa un menor nivel de cumplimiento de la normativa de protección de datos, ya que en un 32,5% de centros esta actuación no se lleva a cabo. En un 85,6% de los centros que realizan la auditoría, se han detectado en ella deficiencias de seguridad.

Un 22,5% de los hospitales han realizado la última auditoría en 2010, un 30,8% en 2009, un 10% en 2008 y un 7,4% en 2006 o años anteriores. Un 29,3% de los centros no aporta información sobre la fecha de la última auditoría de seguridad realizada.

Por otra parte, es de destacar que la gran mayoría de centros hospitalarios (82%) optan de manera total o parcial por un auditor externo para la realización de la auditoría de seguridad.

5. RESULTADOS POR TITULARIDAD DEL CENTRO HOSPITALARIO

Los resultados del requerimiento informativo remitido por la AEPD a los centros hospitalarios indican en general un mayor nivel de cumplimiento de la normativa de protección de datos en los centros privados. Las mayores diferencias se observan en los siguientes apartados:

- En materia de inscripción de ficheros, un 99% de los centros privados han cumplido con este requisito normativo, frente al 89% de los centros públicos. La diferencia aumenta cuando se requiere sobre el mantenimiento y actualización de la inscripción, que se lleva a cabo en el 96% de los hospitales privados frente a un 80% de los públicos.

- En el caso de centros públicos, el porcentaje de hospitales que ha publicado la disposición general de creación del fichero en el diario oficial correspondiente es ligeramente inferior al de hospitales que han inscrito sus ficheros en el RGPD: 83,8% frente a 89,1% respectivamente. Esta pequeña diferencia obedece al hecho de que algunos hospitales no han modificado la primera inscripción realizada de manera centralizada por el Ministerio de Sanidad y Consumo en 1994 como consecuencia de la entrada en vigor de la Ley Orgánica 5/1992, de 29 de octubre, de Tratamiento Automatizado de los Datos de carácter personal (LORTAD), antes de realizar las transferencias de sanidad a la mayoría de comunidades autónomas. Si bien posteriormente la Agencia ha modificado de oficio el responsable del fichero, en un número reducido de casos no se ha realizado una nueva publicación del fichero en el diario oficial correspondiente por parte del hospital o del centro gestor competente de la Comunidad Autónoma.

- Mientras que el 94,5% de los centros privados han incluido en los formularios de recogida de datos una cláusula informativa conforme al artículo 5 de la LOPD y el 80% de ellos dispone de carteles informativos sobre el derecho de protección de datos personales a disposición de los usuarios, estos porcentajes descienden al 55% y al 64% respectivamente en el caso de los centros públicos.

- En relación con el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, el 96% de los centros privados cuentan con procedimientos para su atención efectiva, frente al 84% de los centros públicos.

- Un 98% de los centros privados y un 83% de los centros públicos han elaborado el Documento de Seguridad previsto en el reglamento de la LOPD.

- En el caso de los hospitales privados el 85,6% mantiene un registro de todos los accesos a la información, aunque solamente el 79% almacena este registro por un periodo mínimo de dos años, y el 65% audita que los accesos han sido realizados por personal autorizado que los ha utilizado para la finalidad que justificó su acceso.

- Por otra parte, el 62,6% de los hospitales públicos dispone de este registro de accesos, el 58% lo mantiene por un periodo mínimo de dos años y en el 25% de los casos se auditan estos accesos.

- El 95% de los centros hospitalarios privados cuentan con un procedimiento para la notificación y gestión de las incidencias de seguridad, frente al 80,4% de los centros de titularidad pública.

- En el 89,4% de los hospitales privados los dispositivos de almacenamiento de las historias clínicas cuentan con mecanismos que obstaculizan su apertura (por ejemplo, archivadores con cerradura), descendiendo este porcentaje al 65,3% en el caso de los públicos.

- El 86% de los hospitales privados han adoptado medidas para evitar la sustracción, pérdida o acceso indebido a la documentación durante su transporte (ej. traslado de las historias clínicas), frente al 70% de los hospitales públicos.

- En el 94% de los centros privados se ha informado al personal de limpieza sobre la necesidad de garantizar la confidencialidad de los datos (por ejemplo, en la recogida de la basura), mientras que este porcentaje es del 74% en el caso de centros públicos.

- Una de las mayores diferencias se produce en la realización de la auditoría bienal de seguridad del fichero de historias clínicas, requisito que es cumplido por el 88% de los hospitales privados frente a un 44% de los públicos.

Por el contrario, se observa una mayor implantación de la Historia Clínica Electrónica en los centros públicos, con un porcentaje del 66,8% frente al 44,3% de los privados.

Es importante asimismo destacar que la contratación o externalización del tratamiento de los datos está ampliamente implantada tanto en los centros públicos (83,4%) como en los privados (88,3%). En ambos casos, no obstante, el porcentaje de centros en los que se aplican procedimientos de disociación de los datos personales en los servicios externalizados es bajo (44% en centros públicos y 35% en centros privados).

6. RESULTADOS POR COMUNIDADES AUTÓNOMAS

Con carácter general, se observa un alto nivel de cumplimiento de la normativa de protección de datos en las comunidades autónomas de La Rioja y Murcia. En el resto de comunidades el comportamiento varía según el concepto analizado:

- Los centros hospitalarios de las CCAA de Aragón (66,67%) y Cantabria (75%) son los que presentan un menor porcentaje de inscripción de ficheros de datos personales en el RGPD. En el resto de comunidades, el promedio de inscripción supera el 87% de centros hospitalarios. Estas mismas comunidades son la que cuentan asimismo con un menor porcentaje de hospitales en los que dicha inscripción se mantiene actualizada: en Aragón es sólo un 41% y un 50% en Cantabria. En ambos parámetros, los indicadores están penalizados por el bajo nivel de cumplimiento en los centros sanitarios de titularidad pública.

- Destaca el bajo nivel de cumplimiento del requisito de publicación de la disposición de creación de ficheros de hospitales de titularidad pública en boletín o diario oficial correspondiente, en las CCAA de Cantabria (25%), Aragón (50%), Canarias (54,5%) y Asturias (58,3%).

- La inclusión de la cláusula informativa conforme al artículo 5 de la LOPD en los formularios de recogida de datos de los pacientes es particularmente baja en los hospitales públicos de Aragón (5%), Castilla y León (23%), Asturias (25%), Canarias (27%) y Galicia (32%).

- La disponibilidad de procedimientos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición supera el 75% de los hospitales en todas las CCAA, a excepción de los centros públicos de las comunidades de Cantabria (50%), Valenciana (62%), Canarias (64%) y Asturias (67%), que se sitúan por debajo de ese umbral.

- La contratación de actividades relacionadas con el tratamiento de datos es mayoritaria en los hospitales de todas las CCAA, a excepción de los centros públicos de Extremadura (50%) y Cantabria (53%) en los cuales esta alternativa de gestión está equilibrada con la gestión 100% interna de los tratamientos de datos.

- Aunque en promedio más del 90% de hospitales cuentan con el documento de seguridad preceptivo según el RLOPD, un 45% de los centros públicos de Canarias y 49% de los de la Comunidad Valenciana no disponen de él.

- En el 55% de los centros públicos de Canarias y en el 45% de los de la Comunidad Valenciana las medidas de seguridad aplicadas a los datos de carácter personal no se corresponden con las de nivel alto según el RLOPD.

- El registro de todos los accesos a la información es particularmente bajo en los hospitales públicos de Extremadura (17,6%), Baleares (27,3%), Aragón (38,9%) y Andalucía (40%).

- Por otra parte, el 55% de los centros públicos de Baleares y Comunidad Valenciana no cuentan con procedimientos para la notificación y gestión de incidencias de seguridad, valor sensiblemente superior al registrado en el conjunto de hospitales de titularidad pública (20%).

- La disponibilidad de dispositivos de almacenamiento de documentos (historias clínicas) que cuenten con mecanismos que obstaculicen su apertura (p.ej. archivadores con cerradura) es particularmente baja en los centros hospitalarios públicos de Cantabria (25%), Galicia (35,5%) y Comunidad Valenciana (48%).

- El nivel de realización de la auditoría bienal de seguridad en los hospitales públicos es muy dispar según la Comunidad Autónoma de que se trate. Así, es particularmente bajo en las comunidades de Castilla y León (7,7%), Asturias (8,3%), Comunidad Valenciana (10,3%), Aragón (16,7%), Canarias (18%) y Cantabria (25%). Por el contrario, es elevado en La Rioja (100%), Galicia (96,8%), Castilla La Mancha (84,2%), Extremadura (82,3%) y Murcia (80%).

7. CONCLUSIONES

El informe de cumplimiento de la normativa de protección de datos ha sido contestado por el 92% de los centros hospitalarios requeridos. En el caso del 8% restante, se ha dado traslado al órgano encargado de la función inspectora y sancionadora dado que podría incurrirse en una infracción conforme al artículo 44.2.b) de la LOPD.

En relación con la muestra de hospitales que han contestado al requerimiento, son de destacar las siguientes conclusiones:

- El cumplimiento de la normativa es alto en el conjunto de centros privados, alcanzándose niveles elevados en la mayoría de conceptos clave analizados: inscripción de ficheros (99%), inclusión de cláusulas informativas en los formularios de recogida de datos (94,5%), disponibilidad de procedimientos para atender el ejercicio de los derechos ARCO (97%) y, en general, en la implantación de medidas de seguridad y su auditoría periódica.

- En promedio, y con excepción de las comunidades de La Rioja y Murcia, el nivel de cumplimiento en los centros públicos es menor que en los centros privados. Las mayores diferencias con éstos se dan en la inclusión de cláusulas informativas en los formularios de recogida de datos (55% frente a 94,5%) y en la realización de la

auditoría bienal de seguridad (45% frente a 88%). Además de las señaladas, las áreas de mejora más importantes son la instalación de carteles informativos sobre el derecho a la protección datos, la revisión periódica del documento de seguridad, el registro de todos los accesos a la información, el archivo de las historias clínicas en dispositivos dotados de mecanismos que obstaculicen su apertura, así como la adopción de medidas para evitar la sustracción, pérdida o acceso indebido a la documentación durante su transporte. Es importante asimismo destacar que en el caso de los hospitales de titularidad pública, los indicadores varían significativamente según el aspecto y comunidad autónoma de que se trate.

- La mayoría de hospitales (86%) han contratado actividades de tratamiento de datos personales. En la práctica totalidad de estos casos se ha incluido en el contrato de prestación de servicios la cláusula informativa prevista en el artículo 12 de la LOPD. Sin embargo, el porcentaje de centros que en este escenario aplican procedimientos de disociación de los datos de carácter personal es todavía bajo (34%).

- La implantación de la Historia Clínica Electrónica alcanza al 55% de los hospitales requeridos, siendo mayor en los centros públicos que en los privados (67% frente a 44%).

8. RECOMENDACIONES

A la luz de los resultados anteriormente expuestos, y sin perjuicio del necesario cumplimiento de todas las obligaciones previstas en la normativa de protección de datos de carácter personal, es necesario hacer especial hincapié en los siguientes aspectos de la misma:

- Mantener actualizada la inscripción de los ficheros de datos de carácter personal.
- En el caso de ficheros de titularidad pública, tener publicada en el diario oficial correspondiente y actualizada la pertinente disposición general de adecuación a la LOPD y al RLOPD
- Incluir en los impresos y formularios de recogida de datos de los pacientes y usuarios cláusulas informativas respecto al tratamiento de datos personales, conforme al artículo 5 de la LOPD, y adaptarlas 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 carteles informativos sobre el derecho a la protección de datos personales de los usuarios del centro, que sean fácilmente visibles por éstos.
- Informar al personal de limpieza sobre la necesidad de garantizar la confidencialidad de los datos (por ejemplo, en la recogida de la basura)

- Es recomendable aplicar procedimientos de disociación de los datos de carácter personal en los tratamientos de datos que hayan sido externalizados.
- Registrar todos los accesos realizados a los historiales clínicos, almacenando la información de cada uno de ellos prevista en el Reglamento de desarrollo de la LOPD durante un periodo no inferior a dos años.
- Realizar auditorías para verificar si el personal autorizado utiliza los datos para la finalidad que justificó el acceso.
- Almacenar los archivos físicos de historias clínicas en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave o dispositivo equivalente. Asimismo, y en el interior de estas áreas, almacenar los expedientes clínicos en archivadores que dispongan de mecanismos que obstaculicen su apertura.
- Custodiar la documentación clínica de pacientes cuando ésta no se encuentre archivada en los dispositivos de almacenamiento indicados en el punto anterior por encontrarse en proceso de revisión o consulta, impidiendo que pueda ser accedida por personas no autorizadas.
- Adoptar medidas para evitar la sustracción, pérdida o acceso indebido a la documentación durante su transporte (ej. traslado de las historias clínicas).
- Realizar la auditoría bienal de seguridad del fichero de historias clínicas y de otros que puedan contener datos relativos a la salud de las personas, adoptando medidas correctoras para subsanar las deficiencias encontradas.

9. ANEXO: RESULTADOS GENERALES DEL INFORME POR TITULARIDAD

Informe de cumplimiento de la LOPD en Hospitales. Resultados

	Centros públicos	Centros privados	TOTAL
¿Se han inscrito los ficheros del Centro Hospitalario en el RGPD?	89,43	98,97	94,42
¿La inscripción se mantiene actualizada?	80,00	95,88	88,31
En el caso de los ficheros de titularidad pública, ¿se ha publicado la disposición general de creación de los ficheros en el diario oficial correspondiente?	83,02	0,00	39,57
Entre las finalidades de los ficheros inscritos en el RGPD, ¿se encuentra la de gestión de Historias Clinicas para asistencia sanitaria?	86,04	94,85	90,65
¿Se ha inscrito un fichero con la finalidad de Investigación Clínica?	55,09	25,77	39,75
¿Se ha inscrito un fichero con la finalidad de Gestión Sanitaria?	83,40	90,03	86,87
¿Se han inscrito los ficheros de Gestión interna del Centro (Recursos humanos, proveedores, etc)?	85,66	93,81	89,93
¿Se han inscrito ficheros con finalidades diferentes de las señaladas en las cuestiones precedentes?	70,94	72,85	71,94
¿En ese Centro se ha implementado la Historia Clínica Electrónica?	66,79	44,33	55,04
En los formularios de recogida de datos de los pacientes y usuarios del Centro, ¿se ha incluido una cláusula informativa conforme a lo establecido en el art. 5 de la LOPD?	55,09	94,50	75,72
¿La cláusula informativa está adaptada 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 ….)?	42,64	82,82	63,67
¿Disponen de carteles informativos sobre el derecho de protección de datos personales a disposición de los pacientes y usuarios del centro?	64,15	80,07	72,48
¿Disponen de procedimientos para atender a las personas que solicitan el ejercicio del derecho de acceso, rectificación, cancelación y oposición?	83,77	96,91	90,65
¿La atención de estos derechos se encuentra centralizada en una Unidad del Centro Hospitalario?	76,60	92,44	84,89
Si se ejerce el derecho a la reserva de las anotaciones subjetivas que constan en la Historia Clínica, ¿la decisión sobre los datos que se facilitan, la toma el profesional sanitario?	76,23	65,29	70,50
El Centro Hospitalario, ¿tiene contratada/externalizada la prestación de servicios de tratamiento de datos personales (custodia de historias clínicas, destrucción de documentos, mantenimiento informático, pruebas analíticas, monitorización de ensayos clínicos, …)?	83,40	88,32	85,97
En los contratos de prestación de servicios, ¿se incluye la cláusula de protección de datos prevista en el art. 12 de la LOPD?	81,51	87,63	84,71
En los servicios externalizados, ¿se aplican procedimientos de disociación de los datos de carácter personal?	36,60	30,93	33,63
¿Se informa al personal de limpieza sobre la necesidad de garantizar la confidencialidad de los datos (por ejemplo, en la recogida de la basura)?	73,96	94,16	84,53
¿Disponen del documento de seguridad previsto en el RLOPD?	83,02	97,94	90,83
¿Se revisa periódicamente el documento de seguridad y, en su caso, se actualiza?	70,19	94,16	82,73
Las medidas previstas en el documento de seguridad, ¿corresponden a las definidas para el nivel alto en el RLOPD?	81,89	94,85	88,67
¿Disponen de medidas técnicas que impidan el acceso de terceros no autorizados o la difusión de datos de carácter personal de los ficheros del centro sanitario (limitación de la descarga de programas de intercambio de archivos, cortafuegos …)?	93,21	96,22	94,78
¿Se encuentran definidas las funciones y obligaciones del personal?	92,45	98,28	95,50
¿El personal conoce sus obligaciones y las normas que tiene que aplicar?	93,21	98,97	96,22
¿Se realizan actividades de formación del personal sobre protección de datos?	74,72	84,19	79,68
El personal que realiza las funciones de facturación y gestión y control sanitario, ¿tiene limitado el acceso a la Historia Clínica?	92,45	84,88	88,49

¿Se encuentra limitado el acceso a los datos y recursos de todo el personal (se impide que los usuarios puedan acceder a datos o recursos distintos de los autorizados)?	94,72	98,63	96,76
¿Se mantiene actualizada una relación de los usuarios que tienen acceso autorizado a los datos personales?	89,81	96,22	93,17
¿Los usuarios se identifican mediante una clave de acceso y una contraseña?	96,23	97,59	96,94
¿Se dispone de un registro de todos los accesos a la información?	62,64	85,57	74,64
En el citado registro, ¿se guardan los datos relativos a la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si se ha autorizado o denegado?	58,11	81,79	70,50
En el citado registro, y en el caso de que el acceso haya sido autorizado, ¿se guarda la información que permite identificar el registro accedido?	59,25	76,98	68,53
¿Se audita si el personal autorizado utiliza los datos para la finalidad que justificó el acceso?	24,91	64,95	45,86
La información del citado registro, ¿se mantiene por un periodo mínimo de 2 años?	58,11	79,04	69,06
¿Se realizan cesiones o comunicaciones de datos?	80,00	79,04	79,50
¿Existe un procedimiento de notificación y gestión de las incidencias de seguridad?	80,38	94,85	87,95
La salida de soportes y documentos fuera del Centro Hospitalario, ¿se encuentran autorizadas?	76,98	84,88	81,12
El procedimiento de realización de copias de respaldo y recuperación de los datos, ¿se encuentra definido?	95,09	97,94	96,58
Los dispositivos de almacenamiento de los documentos (historias clínicas), ¿disponen de mecanismos que obstaculizan su apertura (p.e. archivadores con cerradura)?	65,28	89,35	77,88
Los locales en los que se encuentran los dispositivos de almacenamiento, ¿se encuentran cerrados cuando no hay personal de la organización a su cargo?	94,34	98,63	96,58
¿Se han adoptado medidas para evitar la sustracción, pérdida o acceso indebido a la documentación durante su transporte (ej. traslado de las historias clínicas)?	70,19	86,25	78,60
¿El personal, está informado de su obligación de custodiar la documentación cuando ésta no se encuentra archivada en los dispositivos de almacenamiento por estar en revisión o tramitación?	90,94	97,59	94,42
¿Disponen de medios de destrucción y desecho de la información que garanticen la confidencialidad de la información e imposibiliten su acceso a terceros no autorizados?	92,83	98,97	96,04
¿Se ha realizado la auditoria bienal de seguridad del Fichero de Historias Clínicas?	44,74	88,32	67,50
¿El informe de auditoria indica que se han encontrado deficiencias en la seguridad?	42,86	71,48	57,81
¿La auditoría ha sido realizada por un auditor externo?	34,59	74,23	55,30
¿La auditoría ha sido realizada por un auditor interno?	18,05	17,87	17,95
En el caso de que la auditoría haya sido realizada por un auditor interno, ¿se ha realizado con garantías de independencia?	18,80	19,59	19,21
En su caso, ¿se han adoptado las medidas correctoras relativas a las posibles deficiencias?	40,98	78,69	60,68