

Tras el análisis del cumplimiento de la LOPD de más de 600 centros hospitalarios públicos y privados de toda España

La AEPD detecta importantes deficiencias en el cumplimiento de la protección de datos por los hospitales

- El análisis de la AEPD constata que mientras los centros sanitarios privados presentan índices de cumplimiento elevados, los públicos muestran mayores deficiencias y menores niveles de cumplimiento.
- Los principales incumplimientos se dan en la implantación de medidas de seguridad y custodia de la información, la inclusión de cláusulas informativas en la recogida de datos y la realización de auditorías de seguridad.
- El 30% de los centros públicos carece de medidas para evitar la pérdida o acceso indebido a la documentación clínica durante su transporte, y en el 35% el archivo de las historias clínicas carece de mecanismos que impidan su apertura.
- Cerca del 40% de los centros sanitarios públicos y del 15% de los privados incumplen la obligación de tener un registro de accesos a la información sanitaria.
- Sólo el 55% de los centros públicos incluye cláusulas informativas en los formularios de recogida de datos, frente al 94,5% de los centros privados.
- El 66% de los centros sanitarios públicos no realizan auditoría de seguridad.
- Se constata un elevado nivel de cumplimiento en el conjunto de centros auditados- públicos y privados- en la obligación de inscribir sus ficheros en la AEPD.
- La AEPD ha requerido a más de 200 centros la adopción de medidas correctoras y la comunicación de las mismas a la AEPD en un plazo de 6 meses.
- Se ha dado traslado a la Subdirección de Inspección de la AEPD de los más de 40 centros que no han atendido el requerimiento, dado que podrían haber incurrido en una infracción de la LOPD.

(Madrid, 13 de octubre de 2010). La Agencia Española de Protección de Datos ha hecho público hoy el “*Informe de cumplimiento de la LOPD en Hospitales*” en el que se recogen los resultados y conclusiones del análisis, iniciado por la AEPD el pasado mes de marzo, sobre el nivel de cumplimiento de las garantías de protección de datos en centros sanitarios públicos y privados de toda España.

La evaluación del nivel de cumplimiento de la normativa de protección de datos se ha realizado mediante el envío de un requerimiento de información a **más de 600 centros sanitarios registrados en el Catálogo Nacional de Hospitales**, que se encuentran bajo la competencia de la AEPD, sobre su nivel de cumplimiento de las exigencias recogidas en la Ley Orgánica de Protección de Datos (LOPD), haciendo especial hincapié en la adopción de medidas de seguridad y confidencialidad de la información sanitaria. Cabe destacar que dicho **requerimiento ha sido atendido por el 92% (562 centros)** de los centros hospitalarios requeridos.

Entre las **principales conclusiones** del análisis realizado, en líneas generales se constata un **mayor grado de cumplimiento de la normativa por parte de los centros sanitarios privados respecto a los centros públicos**, en la mayoría de conceptos clave analizados: inscripción de ficheros; inclusión de cláusulas informativas en los formularios de recogida de datos;

disponibilidad de procedimientos para atender el ejercicio de los derechos de los ciudadanos; y en general en la implantación de medidas de seguridad y su auditoría de seguridad periódica.

Asimismo, se pone de manifiesto la existencia en los centros sanitarios públicos (excepto los pertenecientes a las comunidades autónomas de Madrid, Cataluña y País Vasco, por ser competencia éstos de las agencias autonómicas) de **importantes carencias en materia de cumplimiento en la implantación de medidas de seguridad y custodia de la información.**

Además, centro se observa que los centros sanitarios de **Murcia y la Rioja** son los que cuentan con **mayores niveles de cumplimiento**, mientras que los centros ubicados en las comunidades autónomas de Cantabria, Canarias, Valencia y Aragón cuentan con menores índices de cumplimiento de los conceptos analizados.

Según se recoge en el informe las principales conclusiones sobre el **cumplimiento de la LOPD por parte de centros sanitarios** son las siguientes:

1- Deficiente implantación de medidas de seguridad de los datos. La evaluación realizada a los centros sanitarios ha puesto de manifiesto, que pese a que 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, existen centros sanitarios, principalmente públicos, en los que se constatan **importantes deficiencias** en la implantación de medidas **para que los datos personales e información sanitaria de los pacientes sean adecuadamente custodiados y no puedan ser conocidos por terceros no autorizados.** En este sentido el informe destaca los siguientes indicadores:

- Cerca del **35% de los hospitales públicos carecen de mecanismos que obstaculizan la apertura** (por ejemplo, archivadores con cerradura) de los dispositivos de almacenamiento de las historias clínicas en papel, mientras que el 89,4% de los hospitales privados afirma disponer de ellos.
- Se evidencian **deficiencias en la implantación de los registros de acceso a la información.** Esta exigencia de la Ley es cumplida por el 85,6% de los hospitales privados, que manifiestan que se guarda un registro de todos los accesos a la información, y por **un 62,6% de los hospitales públicos.** Asimismo, es de destacar que **sólo el 25% de los centros públicos y 65% de los centros privados** auditan que el personal autorizado utiliza los datos para la finalidad que justificó el acceso a los mismos.
- El **30 %** de los centros sanitarios públicos y cerca del **15 %** de los privados **carecen de medidas para evitar la sustracción, pérdida o acceso indebido a la documentación** durante su transporte (ej. traslado de las historias clínicas).
- Mientras 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), este porcentaje **desciende al 74% en el caso de centros públicos.**
- Una de las mayores diferencias entre públicos y privados se produce en la realización de la **auditoría bienal de seguridad -obligatoria-** del fichero de historias clínicas, requisito que es cumplido tan sólo **44% de los públicos y por el 88% de los hospitales privados.**

2-Carencias en el cumplimiento del deber de información, y atención al ejercicio de derechos de acceso, rectificación, cancelación y oposición. El informe pone de manifiesto que 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 manifiestan que disponen 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 y atención de los derechos** de acceso, rectificación, cancelación y oposición, **un 96% de los centros privados y el 84% de los centros públicos** afirman que cuentan con procedimientos para su atención efectiva.

No obstante, para la AEPD es **destacable** que en los últimos dos años se ha constatado un **incremento significativo en el número de las solicitudes de tutela de derecho relacionadas con el acceso a la historia clínica**. En concreto se **ha experimentado un incremento significativo en las solicitudes de ciudadanos a la AEPD para que tutele su derecho de acceso** al considerar que la historia clínica propia se les ha suministrado de manera incompleta -amparándose los centros sanitarios en el derecho de los facultativos a la reserva de las anotaciones subjetivas en el historial del paciente-, o al serle denegado el acceso al historial clínico de un familiar fallecido.

3- Cumplimiento elevado del deber de inscripción de ficheros en el RGPD. Uno de los únicos indicadores auditados en los que se constata **un elevado nivel de cumplimiento** en el conjunto de centros auditados- públicos y privados- **es la obligación de inscribir sus ficheros en el Registro General de Protección de Datos**. Así, un 99% de los centros privados y un 89% de los centros públicos han cumplido con este requisito normativo. No obstante, la diferencia aumenta cuando se requiere información 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 este ámbito, cabe destacar que los centros hospitalarios de las CC.AA. 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.

-4.Importante presencia de externalización de servicios que implican el tratamiento de datos de pacientes. El informe pone de manifiesto que la externalización de servicios que implican **el tratamiento de datos de los pacientes por entidades distintas al propio centro**, está ampliamente extendida (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 los centros- públicos y privados- por este modelo de gestión.

Cabe destacar que en **la mayoría de los casos los centros han cumplido** con la exigencia normativa -recogida en el artículo 12 de la LOPD- sobre las garantías de “acceso a los datos por cuenta de terceros”, en la que se establece la necesidad de delimitar mediante contrato escrito las finalidades y accesos permitidos, las medidas de seguridad aplicables a los datos personales, así como las responsabilidades en caso de incumplimiento de la normativa.

Es reseñable, sin embargo, que el porcentaje de centros que, en este ámbito, aplican procedimientos de **disociación de los datos** de carácter personal es todavía bajo (34%), ya que si bien no se trata de una obligación exigida por la LOPD, se trata de una práctica recomendable para garantizar la confidencialidad de la información.

Medidas correctoras y subsanación

Para la AEPD las deficiencias detectadas tras la realización de este informe -especialmente las vinculadas al **bajo nivel de cumplimiento de las medidas de seguridad** de la información de los pacientes- son **especialmente preocupantes**, ante los **impactos que el incumplimiento de las garantías de protección de datos por los centros sanitarios puede tener** en la esfera más íntima de los ciudadanos, al tratarse de datos sensibles referidos a la salud de las personas.

En este sentido, **además de introducir en el informe y remitir** a todos los centros sanitarios y Consejerías de Sanidad **un catálogo de recomendaciones y buenas prácticas**, la AEPD **ha realizado un requerimiento a más de 200 centros** que incumplen alguna de las previsiones de la LOPD, al objeto de **que las subsanen** y comuniquen las medidas adoptadas a la institución en **un periodo máximo de 6 meses**.

Asimismo, se ha dado **traslado a la Subdirección General de Inspección de los más de 40 centros que no han atendido el requerimiento de información de la institución**, dado que éstos podrían haber incurrido en una infracción de la LOPD.

Casuística de denuncias e infracciones

La iniciativa de evaluar el nivel de cumplimiento de los centros hospitalarios se debe a **la constatación de alarmantes casos y procedimientos tramitados por la Agencia** vinculados principalmente a la **vulneración de los deberes de seguridad y secreto** por parte de centros sanitarios -entre los que se encuentran casos de **difusión de datos de pacientes a través de redes de intercambio de archivos P2P, como e-Mule, así como datos de salud abandonados en contenedores de la vía pública-** así como al incremento de las **tutelas de derecho relacionadas con el acceso a la historia clínica planteadas por ciudadanos en los últimos años.**

En concreto, en 2009 se registraron **un total de 123 denuncias** y actuaciones previas de investigación en el sector de la sanidad, y en lo que va de 2010 se han registrado cerca de **100** reclamaciones.

Cabe destacar que los principales motivos de denuncias tramitadas por la AEPD provienen de la **aparición de documentación clínica en la vía pública** -historiales clínicos de hospitales públicos y privados, informes de reconocimientos médicos y tarjetas sanitarias- y **almacenamiento de diversa documentación clínica en áreas no restringidas al público** y en dependencias al alcance de cualquiera.

Asimismo, la AEPD ha tramitado diversas reclamaciones relativas a la **pérdida de historiales clínicos de pacientes** al proceder a la automatización de los historiales y no adoptar las medidas de seguridad pertinentes; utilización de los datos sanitarios para finalidades no autorizadas y **la comunicación indebida de datos como comunicación de datos a terceras personas** (caso de entrega de historias o información médica a ex-cónyuges); **entrega de certificados hospitalarios de ingresos a terceras personas con información excesiva**, o denuncias relativas a la cesión de historias clínicas a efectos de facturación a terceras entidades.